



اعتماد استخدام
الامتداد الآمن لأسماء النطاقات
في أسماء النطاقات السعودية

Implementing DNSSEC in
Saudi Domain Names

ICANN60 - Oct 2017

Raed Alfayez, SaudiNIC/CITC

Agenda



فهرس المحتويات

- Roles of CITC/SaudiNIC
- What has been done so far by SaudiNIC
- Lessons learned and the next steps

- دور الهيئة/المركز السعودي لمعلومات الشبكة
- ما تم إنجازه من قبل المركز السعودي لمعلومات الشبكة
- الدروس المستفادة و الخطوات القادمة

Agenda



فهرس المحتويات

- Roles of CITC/SaudiNIC
- What has been done so far by SaudiNIC
- Lesson learned and the next steps

- دور الهيئة/المركز السعودي
لمعلومات الشبكة
- ما تم إنجازه من قبل المركز
السعودي لمعلومات الشبكة
- الدروس المستفادة و الخطوات
القادمة

SaudiNIC is responsible and authorized (by IANA/ICANN) to manage Saudi domain names (.sa, السعودية.)

المركز هو الجهة المسؤولة و المخولة (من قبل آيانا/أيكان IANA/ICANN) بالإشراف على تسجيل أسماء النطاقات السعودية (.sa, السعودية.)

SaudiNIC

- Setting up policies regulating domain name registrations
- Management and Domain name registrations under Saudi ccTLDs
- Maintain the domain names records and provide Whois services
- Lead the effort toward fully Arabic domain names
- International coordination with respect to Saudi ccTLDs.
- Deploying and operating Saudi ccTLD infrastructure

المركز السعودي لمعلومات الشبكة

- وضع اللوائح والقواعد و التنظيمات اللازمة لتسجيل أسماء النطاقات في المملكة العربية السعودية
- الإدارة والإشراف وتسجيل النطاقات السعودية
- توفير قواعد معلومات عن الأسماء المسجلة
- دعم أسماء النطاقات العربية
- التنسيق الدولي فيما يخص النطاقات السعودية
- توفير وتشغيل البنية التحتية لخدمات أسماء النطاقات الوطنية

SaudiNIC

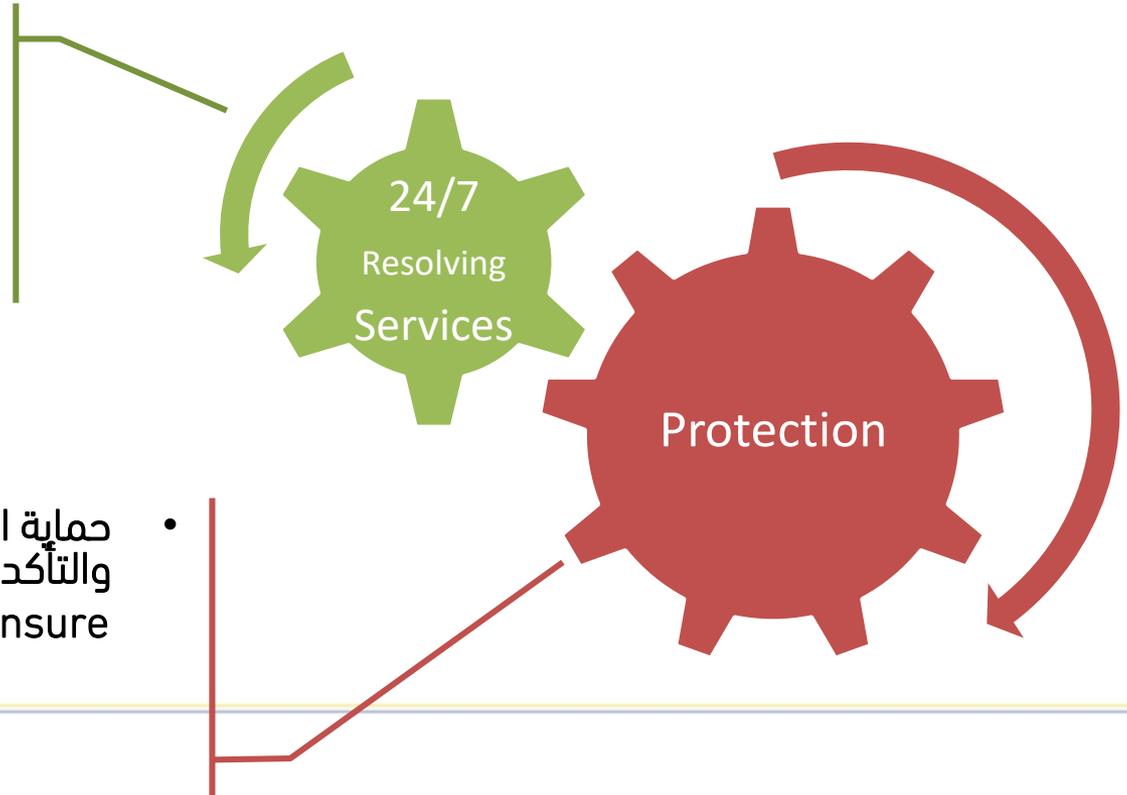
- ...
- Deploying and operating Saudi ccTLD infrastructure

المركز السعودي لمعلومات الشبكة

- ...
- توفير وتشغيل البنية التحتية لخدمات أسماء النطاقات الوطنية

- نشر معلومات التسجيل (لغرض تحويل أسماء النطاقات السعودية إلى العناوين الرقمية)
- Publish Saudi's zone files (Domain names Resolution services)

- حماية البنية التحتية من العبث (الإلكتروني) والتأكد من توفرها على مدى الساعة
- Protect the infrastructure and ensure that it is available 24/7



- **Hidden Primary DNS server**
- **2 copies of the main server on CITC network behind firewalls and secured against DDOS attacks. They are 24/7 monitored.**
- **Multiple secondary servers (local: ISU, STC; worldwide)**
- **About 150 Anycast instances**
- **Promote Local secondary servers (e.g., IXP, Mobily, Zain, ITC, ...)**
- **...**
- **Protection efforts continue where the latest task is DNSSEC**

وجود خادم أساسي مخفي (لا يمكن الوصول إليه من خلال شبكة الإنترنت)

وضع نسختين للخادم الأساسي على شبكة الهيئة وتأمينها بعدة أجهزة حماية (Firewalls) مع تأمينها أيضا ضد هجمات التعطيل (DDOS) ووضعها تحت أجهزة الرقابة على مدار الساعة

نشر عدة نسخ ثانوية محليا (الهيئة، مدينة الملك عبدالعزيز للعلوم والتقنية، شركة الاتصالات السعودية) ودوليا (أوروبا، أمريكا، وأستراليا) استخدام تقنية (anycast) لغرض التوزيع الجغرافي للحد من هجمات تعطيل الخدمة (DOS attacks) .. حوالي 10٠ نسخة موزعة حول العالم

العمل جاري لإيجاد نسخ محلية أخرى لدى المشغلين المحليين (مثل المقسم الوطني، موبيلي، زين، الاتصالات المتكاملة، ...)

والعمل مستمر لحماية البنية التحتية، ومن آخر الخطوات الامتداد الآمن لنظام أسماء النطاقات (DNSSEC)



Agenda



فهرس المحتويات

- Roles of CITC/SaudiNIC
- What has been done so far by SaudiNIC
- Lesson learned and the next steps

- دور الهيئة/المركز السعودي لمعلومات الشبكة
- ما تم إنجازه من قبل المركز السعودي لمعلومات الشبكة
- الدروس المستفادة و الخطوات القادمة

What has been done so far



ما تم إنجازه من قبل المركز حتى الآن

2015

مرحلة الدراسة Studying Phase

- تجارب الدول
- المواصفات الدولية

- Country case studies
- International standards

- التعلم من أخطاء الآخرين
- انتظار نضوج التقنية

- Learning from others' mistakes
- Waiting for application maturity and availability of tools

مرحلة المتابعة Follow up Phase

Before
2015

- أولاً: كسب الخبرة المحلية
- ثانياً: التشغيل التجريبي
- ثالثاً: التشغيل الفعلي

- Stage I: Gaining and building local expertise.
- Stage II: Prototype and experimental operation.
- Stage III: Launching the actual operation.

مرحلة التنفيذ

Execution Phase

2016-2017

What has been done so far



ما تم إنجازه من قبل المركز حتى الآن

- 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).

• البدء بخطى متزنة ومتروية

- المتابعة المستمرة للتطورات الدولية
- لماذا التريث

- التغيير السريع للمواصفات حتى هذه اللحظة
- انتظار نضج التطبيقات و توفر الأدوات
- الاستفادة من خبرة وتجارب الآخريين 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



ما تم إنجازه من قبل المركز حتى الآن

- 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.

- 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.

DNSSEC adoption methodology



منهجية تبني الامتداد الآمن

- Counted on its **national staff** in R&D and in building systems.
- **Trained** some of our staff by attending DNSSEC courses and workshops.
- Established a number of **relationships** with DNSSEC international **experts**.
- Conducted some **studies**, develop operational **plans**, prepare technical and **procedural** policy documents, determine requirements, and then execute implementations.
- Implementing the project in stages and internally by SaudiNIC employees relying - after God - on the **open source software** environment

- الاعتماد على الأيدي الوطنية للبحث والتطوير وبناء الأنظمة
- تأهيل بعض منسوبيه لحضور بعض الدورات وورش العمل ذات العلاقة
- تكوين العلاقات مع المختصين وذوي الخبرات الدولية في هذا المجال
- القيام ببعض الدراسات ووضع الخطط التنفيذية وإعداد الضوابط الفنية والإجرائية وتحديد المتطلبات وتنفيذها
- تنفيذ المشروع على مراحل داخليا من قبل منسوبي المركز السعودي لمعلومات الشبكة معتمدين - بعد الله - على بيئة البرمجيات مفتوحة المصدر.

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)
 - موجهة لموظفي الهيئة في المركز السعودي لمعلومات الشبكة والمختصين في القطاع
 - ٢٥ مشارك يمثلون ١١ جهة 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

- وثيقة ممارسات المركز
- إعداد التصاميم وطريقة العمل
- وثيقة إجراءات الامتداد الآمن
- تحديد الصلاحيات
- خطة إدارة المخاطر

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 from 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 يحملها 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). وتحتد 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 يحدث بها أثناء انتقالها خلال شبكة الإنترنت وأنها آتية من مصدرها الصحيح. ويتحقق ذلك من خلال تبني المفاتيح العامة للتشفير ضمن هيكلية خدمة أسماء النطاقات لتشكل سلسلة موثوقة نابذة من منطقة الجذر (root zone).

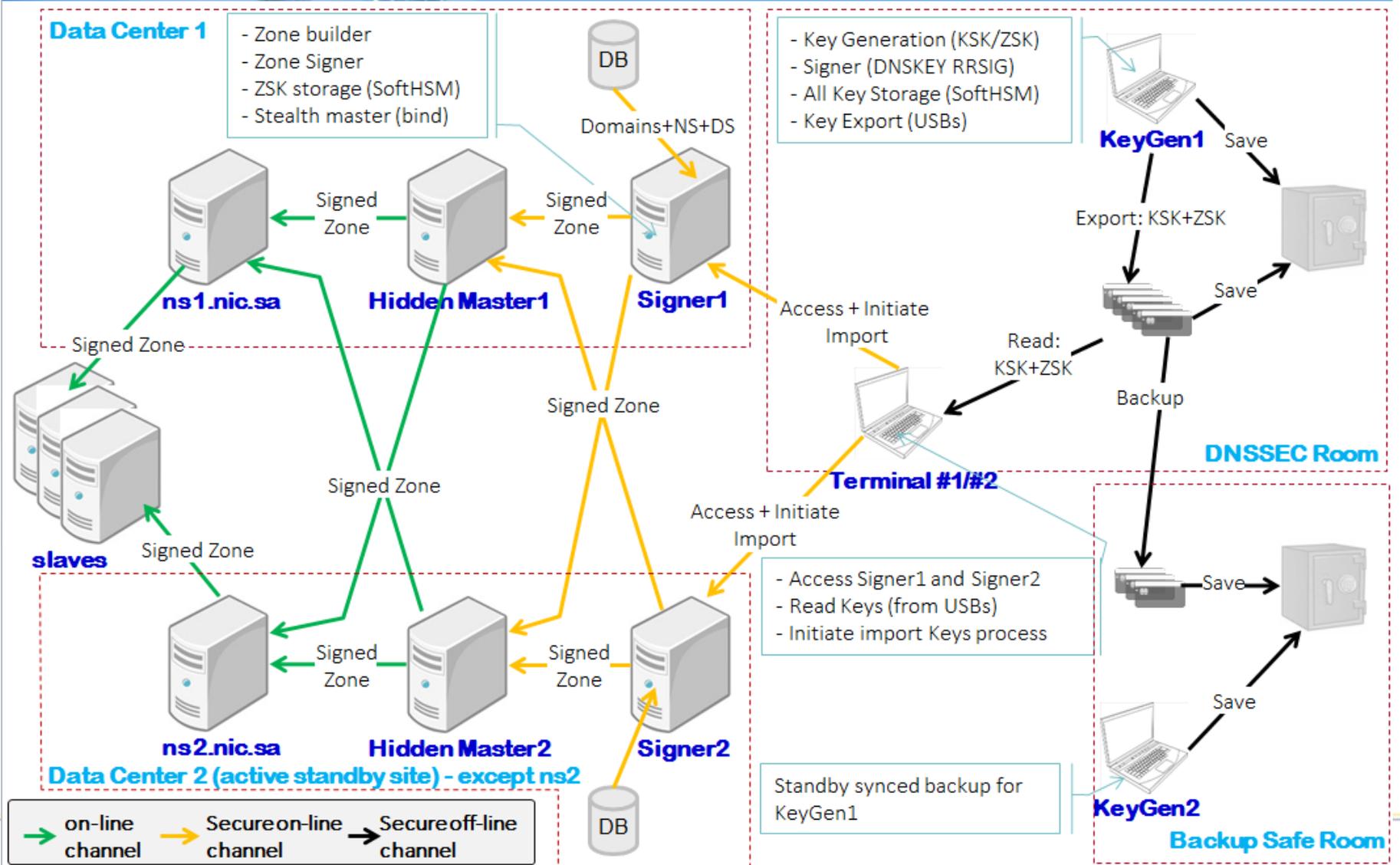
1.2 التعريف واسم الوثيقة

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 خزانة جديدة
- DNSSEC New Safe Arrangement Procedure
- إجراءات نقل مواد من خزانة
- 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 (٢٢ يونيو 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

Key Generation Ceremony

مراسيم إنشاء المفاتيح **!sa**



SaudiNIC DNSSEC CEREMONY SCRIPT
1.1.1 - 06 Jun 2017

Roles	Description	Abbreviations	Description
SM	SaudiNIC Manager	ISIC	Saudi Network Information Center
DSS	DNSSEC Specialist	GUI	Graphical User Interface
SA	System Administrator	HSM	Hardware Security Module
WI	Witness 1,2	SKM	Key Signing Key
		ZSK	Zone Signing Key
		DS	Delegation Signature
		TEB	Timestamp Evident Bag

Participants		
Title	Full Name	Signature
SM	Raoud AlFagez	
DSS	Abdullah AlShammari	
SA	Ahmed AlKhatib	
WI	Abdulwazir H. Al-Zaman	
WI	Nasser S. AlHijab	
WI	Anas Assiri	
SM	Ibrahim AlTurabi	
WI	Ali Alshahr	
WI	Majed S. Alomran	
WI	Fahad S. Alaydi	
WI	Hasham Al-Hamad	
DSS	Solih Alqatani	
DSS	Fahad Alshahr	
SM	Sulaiman Mudad	

1.1.1 - 06 Jun 2017
SaudiNIC DNSSEC ceremony script

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

DS Record Generator

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

Domain Information

Domain Name



Captcha

DNSKEY Record Information

Flags

Protocol

Key algorithm

Public key

DS Record Information

Agenda



فهرس المحتويات

- Roles of CITC/SaudiNIC
- What has been done so far by SaudiNIC
- Lesson learned and the next steps

- دور الهيئة/المركز السعودي لمعلومات الشبكة
- ما تم إنجازه من قبل المركز السعودي لمعلومات الشبكة
- الدروس المستفادة و الخطوات القادمة

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 السيناريوهات)
- 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

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

- 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



Thank you

شكرًا

للمزيد من المعلومات يمكنكم زيارة:

For more information you can visit:



المركز السعودي لعلومات 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