ITPC MANAGEMENT'S ASSERTION

Informatics & Telecommunications Public Company as the National Root Certification Authority of Iraq ("ITPC") has deployed a public key infrastructure.

As part of this deployment, it was necessary to create a hierarchy consistent of self-signed Root CAs known as ITPC Document Signing Root CA G1, ITPC CS Root CA G1, ITPC SMIME Root CA G1, ITPC TLS Root CA G1 and ITPC TSA Root CA G1 (collectively, "ITPC Root CAs"). These CA's will serve as Root CAs for client certificate services. In order to allow the CA's to be installed in a final production configuration, a Root Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the CA's private signing key. This helps assure the non-refutability of the integrity of the ITPC Root CAs' key pairs, and in particular, the private signing keys.

ITPC management has securely generated key pairs, each consisting of a public and private key, in support of its CA operations. The key pairs were generated in accordance with procedures described in IRAQ National PKI ITPC National Root CA Certification Policy and Certificate Practice Statement, and its Root Key Generation Scripts, which are in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

ITPC management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the root key generation process.

ITPC management is responsible for establishing and maintaining procedures over its CA root key generations, and over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the ITPC Root CAs, and for the CA

تأييد عن سلطة التصديق للشركة العامة للاتصالات والمعلوماتية

إنّ الشركة العامة للاتصالات والمعلوماتية الوطنية في العراق قامت بنشر بنية تحتية للمفتاح العام.

وكجزءٍ من هذا النشر،كان من الضروري إنشاء هيكل هرمي يتكون من سلطات تصديق جذرية موقعة ذاتياً تُعرف باسم الجيل الأول للشركة العامة للاتصالات والمعلوماتية لتوقيع الوثائق ومنها الجيل الأول لسلطة التصديق الجذرية لتوقيع الخوارزميات والجيل الأول للشركة العامة للاتصالات والمعلوماتية لتوقيع البريد الإلكتروني الآمن SMIME والجيل الأول لسلطة التصديق الجذرية لتأمين الاتصالات والجيل الأول للشركة العامة للاتصالات والمعلوماتية للختم الزمني (ويُشار إليها مجتمعة باسم السلطات الجذرية للشركة العامة للاتصالات والمعلوماتية). وستعمل هذه السلطات كسلطات تصديق جذرية لخدمات شهادات العملاء. ولضمان تثبيت هذه السلطات في التكوين النهائي للإنتاج، تم إجراء مراسم توليد المفتاح الجذري، والتي تهدف إلى الإشراف الرسمي على إنشاء المفتاح الخاص لتوقيع سلطات التصديق وتوثيقه. ويساعد ذلك في ضمان عدم إمكانية إنكار سلامة أزواج مفاتيح السلطات الجذرية للشركة العامة للاتصالات والمعلوماتية، لا سيما مفاتيح التوقيع الخاصة.

أنشأت إدارة الشركة العامة للاتصالات والمعلوماتية أزواج مفاتيح بشكل آمن، كل منها يتكون من مفتاح عام وخاص، لدعم عمليات سلطات التصديق الخاصة بها. وُلدت أزواج المفاتيح وفقاً للإجراءات الموضحة في سياسة الشهادات وبيان ممارسات الشهادات للشركة العامة للاتصالات والمعلوماتية الوطنية في العراق، وكذلك وفقاً لنصوص توليد المفاتيح الجذرية الخاصة بها، والتي تتماشى مع معيار ٤,١ لتوليد مفاتيح سلطات التصديق وفقاً لمبادئ ومعايير ويب تراست لسلطات التصديق الإصدار ٢,٢,٢.

كما وضعت إدارة الشركة العامة للاتصالات والمعلوماتية ضوابط فعالة على عملية توليد هذه المفاتيح وحافظت عليها. صُممت هذه الضوابط لتوفير مستوى معقول من التأكيد على الالتزام بالممارسات المذكورة أعلاه طوال عملية توليد المفتاح الجذري.

وإنّ إدارة الشركة العامة للاتصالات والمعلوماتية مسؤولة عن وضع وصيانة الإجراءات الخاصة بتوليد المفاتيح الجذرية لسلطات التصديق الخاصة بها، وضمان سلامة وسرية جميع المفاتيح الخاصة ومفاتيح الوصول (بما في ذلك المفاتيح الفعلية والرموز المميزة وكلمات المرور) المستخدمة في إنشاء سلطات التصديق الجذرية الوطنية،

environment controls relevant to the generation and protection of its CA keys.

وكذلك عن الضوابط البيئية ذات الصلة بتوليد وحماية مفاتيح سلطات التصديق الخاصة بها.

ITPC management has assessed the procedures and controls for the generation of the CA keys. Based on that assessment, in management's opinion, in generation and protecting its CA keys for the ITPC Root CA's between 2024-06-02 and 2024-06-13 at Baghdad, Iraq, with the following identifying information:

كما قيّمت إدارة الشركة العامة للاتصالات والمعلوماتية الإجراءات والضوابط الخاصة بتوليد مفاتيح سلطات التصديق. وبناءً على هذا التقييم ترى الإدارة أنه فيما يخص توليد وحماية مفاتيح سلطات التصديق الجذرية الوطنية خلال الفترة من ٠٢-٠٦-٢٠٢٤ إلى ١٣-٠٦-٢٠٢٤ في بغداد، العراق بالمعلومات التعريفية التالية:

Root Name	Subject Key Identifier	Certificate Serial Number
ITPC Document Signing Root CA G1	50140A374CB812B34F6675BBA97D6E07BE901165	151002928E9A8167BBCFD964CFFDD9C5
ITPC CS Root CA G1	F4F3A9DCC5D272FBA6B000569EBE7695625D6C0A	4446DA0F940BDA93758D706EA7A982D7
ITPC SMIME Root CA G1	A50E9B28736E57E0490F85AD8408456A9562ED4F	58C1BA96BB20CB9AE97D0077CE782B54
ITPC TLS Root CA G1	1628C29875684881BCDC88840C28480CC5EB2DDB	6D1A853A5089AF8739345C4C911EA672
ITPC TSA Root CA G1	80DD81FAFB188610FB7BEF69ADCBBF390A5ECDF7	6C2CB0BA8B3FB2EBEF4B71ABBCE5303B

ITPC has:

- Followed the CA key generation and protection requirements in its:
  - IRAQ National PKI ITPC National Root CA Certification Policy and Certificate Practice Statement, version 1.1 as of 2024-05-28.
- Included appropriate, detailed procedures and controls in its Root Key Generation Scripts:
  - Iraq National PKI – Key Generation Scripts, version 1.0 as of 2024-05-23,
  - Iraq National PKI – Key Generation Ceremonies Exceptions, version 1.0 as of 2024-07-11,
- Maintained effective controls to provide reasonable assurance that the ITPC Root CAs were generated and protected in conformity with the procedures described in its CP/CPS and its Root Key Generation Scripts.

اتبعت الشركة العامة للاتصالات والمعلوماتية ما يلي:

- متطلبات إنشاء وحماية مفاتيح سلطات التصديق وفقاً لما ورد في:
  - سياسة الشهادات وبيان ممارسات الشهادات للشركة العامة للاتصالات والمعلوماتية الوطنية في العراق، الإصدار ١,١ بتاريخ ٢٨-٠٥-٢٠٢٤
- إدراج إجراءات وضوابط مفصلة ومناسبة في نصوص توليد المفاتيح الجذرية:
  - نصوص توليد المفاتيح للبنية التحتية الوطنية للمفتاح العام في العراق-٠٥-٢٠٢٤، الإصدار ١,٠ بتاريخ ٢٣
  - استثناءات حفل توليد المفاتيح للبنية التحتية الوطنية للمفتاح العام في العراق، الإصدار ١,٠ بتاريخ ١١-٠٧-٢٠٢٤
- الحفاظ على ضوابط فعالة لضمان توفير مستوى معقول من التأكيد بأن سلطات التصديق الجذرية الوطنية قد تم إنشاؤها وحمايتها وفقاً للإجراءات الموضحة في سياسة الشهادات وبيان ممارسات الشهادات ونصوص توليد المفاتيح الجذرية الخاصة بها.

- Performed, during the root key generation process, all procedures required by the Root Key Generation Scripts.
- Generated the CA keys in a physically secured environment as described in its CP/CPS.

- تنفيذ جميع الإجراءات المطلوبة أثناء عملية توليد المفتاح الجذري، كما هو محدد في نصوص توليد المفاتيح الجذرية.
- إنشاء مفاتيح سلطات التصديق في بيئة محمية مادياً وفقاً لما هو موضح في سياسة الشهادات وبيان ممارسات الشهادات.

- Generated the CA keys using personnel in trusted roles under multiple person control and split knowledge.
- Generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

- إنشاء مفاتيح سلطات التصديق باستخدام أفراد في أدوار موثوقة تحت إشراف متعدد وتحكم مقسم للمعرفة.
- إنشاء مفاتيح سلطات التصديق داخل وحدات تشفير تلبي المتطلبات التقنية والتجارية المعمول بها وفقاً لما هو موضح في سياسة الشهادات وبيان ممارسات الشهادات، ووفقاً لمعيار ٤,١ لتوليد مفاتيح سلطات التصديق من مبادئ ومعايير ويب تراست لسلطات التصديق، الإصدار ٢,٢,٢.

Ali Yaseen Dawood

ITPC PMA Head
03-07-2024

علي ياسين داوود

رئيس سلطة إدارة التوقيع الإلكتروني
٢٠٢٤-٠٧-٠٣