Ministry of Communications
Informatics & Telecom Public Company
Directorate of Information

وزارة الأتصالات
الشركة العامة للأتصالات والمعلوماتية
مديرية المعلوماتية

ITPC

ITPC MANAGEMENT'S ASSERTION

ITPC Certification Authority ("ITPC") operates the National PKI of Iraq Root Certification Authority (CA) services as enumerated in Amendment A and provides the following CA services:

- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA [cross-] certification

The management of ITPC is responsible for establishing controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, controls placed into operation can only provide reasonable assurance with respect to ITPC Certification Authority operations.

ITPC management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in ITPC management's opinion, in providing its Certification Authority (CA) services at Baghdad, Iraq, as of 2024-07-03, ITPC has:

- Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - IRAQ National PKI ITPC National Root CA Certification Policy and Certificate Practice Statement, version 1.1 as of 2024-05-28,

تأييد عن سلطة التصديق للشركة العامة للاتصالات والمعلوماتية

سلطة التصديق للشركة العامة للاتصالات والمعلوماتية تقوم بتشغيل خدمات سلطة التصديق الجذرية للبنية التحتية للمفتاح العام الوطني العراقي كما هو مذكور في التعديل أ ، وتوفر الخدمات التالية لسلطة التصديق:

- إعادة إصدار الشهادات
- إصدار الشهادات
- توزيع الشهادات
- إبطال الشهادات
- التحقق من صحة الشهادات
- التصديق المتبادل للجهات التابعة لسلطة التصديق

إنّ إدارة سلطة التصديق للشركة العامة للاتصالات والمعلوماتية مسؤولة عن وضع الضوابط على عمليات سلطة التصديق، بما في ذلك الإفصاح عن ممارسات سلطة التصديق على موقعها الإلكتروني، وإدارة ممارسات أعمال سلطة التصديق، وضوابط البيئة الخاصة بها، وضوابط إدارة دورة حياة مفاتيح سلطة التصديق، وضوابط إدارة دورة حياة مفاتيح المشتركين، وضوابط إدارة دورة حياة الشهادات، وضوابط إدارة دورة حياة شهادات الجهات التابعة لسلطة التصديق. تتضمن هذه الضوابط آليات مراقبة، ويتم اتخاذ الإجراءات اللازمة لتصحيح أي أوجه قصور يتم تحديدها.

كما أنّ هناك قيود متأصلة في أي ضوابط بما في ذلك احتمال حدوث خطأ بشري والتحايل على الضوابط أو تجاوزها. وبناءً على ذلك فإن الضوابط المطبقة يمكنها فقط توفير مستوى معقول من التأكيد فيما يتعلق بعمليات سلطة التصديق للشركة العامة للاتصالات والمعلوماتية.

وقامت إدارة سلطة التصديق للشركة العامة للاتصالات والمعلوماتية بتقييم الإفصاحات الخاصة بممارسات الشهادات والضوابط المتعلقة بخدمات سلطة التصديق. بناءً على هذا التقييم ترى إدارة سلطة التصديق للشركة العامة للاتصالات والمعلوماتية أنه عند تقديم خدمات سلطة التصديق في بغداد، العراق اعتباراً من ٢٠٢٤-٧-٠٣ ، فإن سلطة التصديق للشركة العامة للاتصالات والمعلوماتية قد:

- أفصحت عن ممارساتها المتعلقة بالأعمال وإدارة دورة حياة المفاتيح وإدارة دورة حياة الشهادات وضوابط البيئة الخاصة بسلطة التصديق في:
  - سياسة الشهادات وبيان ممارسات الشهادات لسلطة التصديق الوطنية للشركة العامة للاتصالات والمعلوماتية العراقية ضمن البنية

Baghdad – Al- Sadon Street – nearby Baghdad Hotel
Tel:- 7177780
Email: - dgoffice@itpc.gov.iq
Website: - www.itpc.gov.iq

بغداد – شارع السعدون- قرب فندق بغداد
للأتصال: - ٧١٧٧٧٨٠
البريد الألكتروني: -dgoffice@itpc.gov.iq
www.itpc.gov.iq

التحتية للمفتاح العام الوطني العراقي، الإصدار ١.١ بتاريخ ٢٨-٠٥-٢٠٢٤

- سياسة الشهادات لمزودي خدمات التصديق ضمن البنية التحتية للمفتاح العام الوطني العراقي، الإصدار ٢.١ بتاريخ ٣١-٠٥-٢٠٢٤

- Iraq National PKI Certificate Policy (CP) for Trust Services Providers (TSPs), version 1.2 as of 2024-05-31,

- قامت بتصميم الضوابط بشكل مناسب ووضعها قيد التنفيذ لتوفير مستوى معقول من التأكيد بأن:
  - سلطة التصديق للشركة العامة للاتصالات والمعلوماتية تقدم خدماتها وفقاً لبيان ممارسات الشهادات الخاص بها.

- Suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - ITPC provides its services in accordance with its Certification Practice Statement,

- صُمِّمت الضوابط بشكلٍ مناسبٍ ووُضِعَت قيد التنفيذ لتوفير مستوى معقولٍ من التأكيد بأن:
  - سلامة المفاتيح والشهادات التي تديرها سلطة التصديق للشركة العامة للاتصالات والمعلوماتية يتم تأسيسها وحمايتها طوال دورة حياتها.
  - سلامة مفاتيح المشتركين وشهاداتهم التي يديرها مزودو خدمات التصديق المرخَّص لهم يتم تأسيسها وحمايتها طوال دورة حياتها.
  - يتم التحقق من هوية المشتركين بشكلٍ صحيح بالنسبة لأنشطة التسجيل التي يجريها مزودو خدمات التصديق المرخَّص لهم.
  - طلبات شهادات الجهات التابعة لسلطة التصديق تكون دقيقة وموثقة ومعتمدة.
- كما صُممت الضوابط بشكل مناسب ووُضعت قيد التنفيذ لتوفير مستوى معقول من التأكيد بأن:
  - الوصول المنطقي والمادي إلى أنظمة سلطة التصديق وبياناتها مقيد بالأفراد المخول لهم.
  - استمرارية عمليات إدارة المفاتيح والشهادات محفوظة.
  - تطوير وصيانة وتشغيل أنظمة سلطة التصديق يتم تفويضها وتنفيذها بشكل صحيح للحفاظ على سلامة أنظمة سلطة التصديق وفقاً لمبادئ ومعايير ويب ترست لسلطات التصديق الإصدار ٢.٢.٢، بما في ذلك ما يلي:

- Suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - The integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - The integrity of subscriber keys and certificates managing by licensed TSPs is established and protected throughout their lifecycles;
  - Subscriber information is properly authenticated (for the registration activities performing by the licensed TSPs); and
  - Subordinate CA certificate requests are accurate, authenticated, and approved;
- Suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data is restricted to authorized individuals;
  - The continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2, including the following:

الإفصاح عن ممارسات أعمال سلطة التصديق

- بيان ممارسات الشهادات وسياسة الشهادات

CA Business Practices Disclosure

- Certification Practice Statement and Certificate Policy (CP/CPS)

إدارة ممارسات أعمال سلطة التصديق

- إدارة سياسة الشهادات وبيان ممارسات الشهادات

CA Business Practices Management

- Certificate Policy/Certification Practice Statement Management

ضوابط البيئة الخاصة بسلطة التصديق

CA Environmental Controls

Ministry of Communications
Informatics & Telecom Public Company
Directorate of Information

وزارة الأتصالات
الشركة العامة للأتصالات والمعلوماتية
مديرية المعلوماتية

ITPC

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

- إدارة الأمان
- تصنيف الأصول وإدارتها
- أمن الأفراد
- الأمن المادي والبيئي
- إدارة العمليات
- إدارة الوصول إلى الأنظمة
- تطوير الأنظمة وصيانتها
- إدارة استمرارية الأعمال
- المراقبة والامتثال
- تسجيل التدقيق

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

ضوابط إدارة دورة حياة مفاتيح سلطة التصديق

- توليد مفاتيح سلطة التصديق
- تخزين مفاتيح سلطة التصديق
- توزيع المفتاح العام لسلطة التصديق
- استخدام مفاتيح سلطة التصديق
- أرشفة وإتلاف مفاتيح سلطة التصديق
- التعرض لمخاطر اختراق مفاتيح سلطة التصديق
- إدارة دورة حياة الأجهزة التشفيرية الخاصة بسلطة التصديق

Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

ضوابط إدارة دورة حياة مفاتيح المشتركين

- متطلبات إدارة مفاتيح المشتركين

Certificate Lifecycle Management Controls

- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

ضوابط إدارة دورة حياة الشهادات

- إعادة إصدار الشهادات
- إصدار الشهادات
- توزيع الشهادات
- إبطال الشهادات
- التحقق من صحة الشهادات

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

ضوابط إدارة دورة حياة شهادات الجهات التابعة لسلطة التصديق

- إدارة دورة حياة شهادات الجهات التابعة لسلطة التصديق

ITPC does not escrow its CA keys, does not provide subscriber key generation and subscriber certificate issuance services, and does not provide certificate renewal and suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

لا تقوم الشركة العامة للاتصالات والمعلوماتية (ITPC) بحفظ مفاتيح سلطة التصديق عند طرف ثالث كوديعة، ولا تقدم خدمات توليد مفاتيح المشتركين أو إصدار شهاداتهم، كما أنها لا تقدم خدمات تجديد أو تعليق الشهادات. وبالتالي، لم تمتد إجراءاتنا إلى الضوابط التي قد تتعلق بتلك المعايير.

Ali Yaseen Dawood

ITPC PMA Head
03-07-2024

علي ياسين داوود

رئيس سلطة إدارة التوقيع الإلكتروني
٢٠٢٤-٠٧-٠٣

Baghdad – Al- Sadon Street – nearby Baghdad Hotel
Tel:- 7177780
Email: - dgoffice@itpc.gov.iq
Website: - www.itpc.gov.iq

بغداد – شارع السعدون- قرب فندق بغداد
للأتصال: - ٧١٧٧٧٨٠
البريد الألكتروني: -dgoffice@itpc.gov.iq
الموقع الألكتروني :-www.itpc.gov.iq

Amendment A – التعديل أ

Iraq Document Signing Root CA	
Subject	CN=ITPC Document Signing Root CA G1,O=Informatics & Telecommunications Public Company,C=IQ
Serial	151002928E9A8167BBCFD964CFFDD9C5
SHA256 Fingerprint	95750573DC84C0D5FAA6C8EFBCCF5EFC94EEA36C01036D677EF70652CD7EAB67

Iraq Code Signing Root CA	
Subject	CN=ITPC CS Root CA G1,O=Informatics & Telecommunications Public Company,C=IQ
Serial	4446DA0F940BDA93758D706EA7A982D7
SHA256 Fingerprint	F8B4201F4EF588BC5486821D0D7D31EDEBAEBD2F9C61FAACFC9FC980C161570E

Iraq TLS Root CA	
Subject	CN=ITPC TLS Root CA G1,O=Informatics & Telecommunications Public Company,C=IQ
Serial	6D1A853A5089AF8739345C4C911EA672
SHA256 Fingerprint	DA2D6DC502F4F847F66505D1005F4F120FBE5D136A7998AA492189E5741E5FB0

Iraq S/MIME Root CA	
Subject	CN=ITPC SMIME Root CA G1,O=Informatics & Telecommunications Public Company,C=IQ
Serial	58C1BA96BB20CB9AE97D0077CE782B54
SHA256 Fingerprint	DA70509AC9E42DA40E4B4B94D850D3926402F24A30EC332C3A05BA932E86DD46

Iraq Timestamp Root CA	
Subject	CN=ITPC TSA Root CA G1,O=Informatics & Telecommunications Public Company,C=IQ
Serial	6C2CB0BA8B3FB2EBEF4B71ABBCE5303B
SHA256 Fingerprint	442C8E1CCFEB739FB6C5471C3B9491FD24661C958A1BF19B9480C1B3859ED129