

ITPC

ITPC MANAGEMENT'S ASSERTION

ITPC Certification Authority (ITPC) operates the National PKI of Iraq Root Certification Authority (CA) services known as enumerated in Amendment A and provides SSL CA services.

The management of ITPC is responsible for establishing and maintaining effective controls over its SSL CA operations, including its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and SSL 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 SSL CA services. Based on that assessment, in ITPC management's opinion, in providing its SSL Certification Authority (CA) services at Baghdad, Iraq, as of 2024-07-03, ITPC has:

- Disclosed its SSL certificate lifecycle management business practices in its:
 - IRAQ National PKI ITPC National Root CA Certification Policy and Certificate Practice Statement, version 1.1 as of 2024-05-28,
 - Iraq National PKI Certificate Policy (CP) for Trust Services Providers (TSPs), version 1.2 as of 2024-05-31,

Including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the ITPC website, and provided such services in accordance with its disclosed practices;

تأييد عن إدارة سلطة التصديق للشركة العامة للاتصالات والمعلوماتية

إن سلطة التصديق للشركة العامة للاتصالات والمعلوماتية تشغل خدمات سلطة التصديق الجذرية للبنية التحتية للمفتاح العام الوطني العراقي كما هو مذكور في التعديل أ وتوفر خدمات سلطة التصديق للاتصالات الآمنة SSL.

إدارة سلطة التصديق للشركة العامة للاتصالات والمعلوماتية مسؤولة عن إنشاء والحفاظ على ضوابط فعالة لعملياتها في مجال سلطة التصديق للاتصالات الآمنة SSL بما في ذلك الإفصاح عن ممارسات أعمال سلطة التصديق للاتصالات الآمنة SSL على موقعها الإلكتروني وضوابط إدارة دورة حياة مفاتيح الاتصالات الآمنة وضوابط إدارة دورة حياة شهادات الاتصالات الآمنة SSL تتضمن هذه الضوابط آليات مراقبة وتتخذ الإجراءات اللازمة لتصحيح أي أوجه قصور يتم تحديدها.

هناك قيود متأصلة في أي ضوابط بما في ذلك احتمال حدوث خطأ بشري أو التحايل على الضوابط أو تجاوزها وبناءً على ذلك فإن الضوابط الموضوعية قيد التنفيذ لا يمكنها سوى توفير مستوى معقول من التأكيد فيما يتعلق بعمليات سلطة التصديق للشركة العامة للاتصالات والمعلوماتية.

إن إدارة شركة التصديق للشركة العامة للاتصالات والمعلوماتية قامت بتقييم الإفصاحات الخاصة بممارسات الشهادات والضوابط المتعلقة بخدمات سلطة التصديق للاتصالات الآمنة وبناءً على هذا التقييم ترى الإدارة أنه عند تقديم خدمات سلطة التصديق للاتصالات الآمنة SSL في بغداد العراق اعتباراً من ٢٠٢٤-٠٧-٠٣ فإن سلطة التصديق للشركة العامة للاتصالات والمعلوماتية قد:

- أفصحت عن ممارسات أعمال إدارة دورة حياة شهادات الاتصالات الآمنة في:
 - سياسة الشهادات وبيان ممارسات الشهادات لسلطة التصديق الوطنية للشركة العامة للاتصالات والمعلوماتية ضمن البنية التحتية للمفتاح العام الوطني العراقي الإصدار ١,١ بتاريخ ٢٠٢٤-٠٥-٢٨
 - سياسة الشهادات لمزودي خدمات التصديق ضمن البنية التحتية للمفتاح العام الوطني العراقي الإصدار ١,٢ بتاريخ ٢٠٢٤-٠٥-٣١

بما في ذلك التزامها بتوفير شهادات الاتصالات الآمنة SSL بما يتوافق مع متطلبات منتدى سلطات التصديق والمتصفحات على موقع سلطة التصديق للشركة العامة للاتصالات والمعلوماتية الإلكتروني وتقديم هذه الخدمات وفقاً للممارسات المعلنة.

ITPC

- Suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - The integrity of keys and SSL certificates managing by the licensed TSPs is established and protected throughout their lifecycles; and
 - SSL subscriber information is properly authenticated (for the registration activities performing by the licensed TSPs);
- 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 - SSL Baseline v2.8.

ضُمَّتِ الضوابط ونُفِذَتْ بشكل مناسب لتوفير مستوى معقول من التأكيد بأن:

- تأسست وحُفِظَت سلامة المفاتيح وشهادات طبقة المنافذ الآمنة SSL التي يديرها مزودو خدمات التصديق المرخص لهم طوال دورة حياتهم.
- وُثِّقَت معلومات مشتركي طبقة المنافذ الآمنة SSL بشكل صحيح لأنشطة التسجيل المجرة من قبل مزودي خدمات التصديق المرخص لهم.

ضُمَّتِ الضوابط ونُفِذَتْ بشكل مناسب لتوفير مستوى معقول من التأكيد بأن:

- قُيِّد الوصول المنطقي والمادي إلى أنظمة سلطة التصديق وبياناتها بالأفراد المخول لهم
- حُوِّظَ على استمرارية عمليات إدارة المفاتيح والشهادات
- فُوض وطرُور وُضِنَ وشُعِّلَت أنظمة سلطة التصديق بشكل صحيح للحفاظ على سلامة أنظمة سلطة التصديق وفقاً لمبادئ ومعايير ويب ترست لسلطات التصديق لمتطلبات أمان طبقة المنافذ الآمنة الإصدار ٢,٨

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.

Alli Yaseen Dawood

علي ياسين داوود

ITPC PMA Head
03-07-2024

رئيس سلطة إدارة التوقيع الإلكتروني
٢٠٢٤-٠٧-٠٣



ITPC

التعديل أ - Amendment A

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