

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 S/MIME CA services.

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

- Disclosed its S/MIME 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 S/MIME certificates in conformity with the CA/Browser Forum Requirement on the [ITPC website](http://www.itpc.gov.iq), and provided such services in accordance with its disclosed practices;

تأييد عن سلطة التصديق للشركة العامة للاتصالات والمعلوماتية

تُشغل سلطة التصديق للشركة العامة للاتصالات والمعلوماتية خدمات سلطة التصديق الجذرية للبنية التحتية للمفتاح العام الوطني العراقي كما هو مذكور في التعديل أ وتوفر خدمات سلطة التصديق للبريد الإلكتروني الآمن S/MIME.

كما أنّ إدارة سلطة التصديق للشركة العامة للاتصالات والمعلومات مسؤولة عن إنشاء والحفاظ على ضوابط فعالة لعملياتها في مجال سلطة التصديق للبريد الإلكتروني الآمن S/MIME بما في ذلك الإفصاح عن ممارسات أعمال سلطة التصديق للبريد الإلكتروني الآمن S/MIME على موقعها الإلكتروني وضوابط إدارة دورة حياة مفاتيح البريد الإلكتروني الآمن S/MIME وضوابط إدارة دورة حياة شهادات البريد الإلكتروني الآمن S/MIME 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 الموضوعة قيد التنفيذ لا يمكنها سوى توفير مستوى معقول من التأكيد فيما يتعلق بعمليات سلطة التصديق للشركة العامة للاتصالات والمعلوماتية.

كما أنّ إدارة سلطة التصديق للشركة العامة للاتصالات والمعلومات قامت بتقييم الإفصاحات الخاصة بممارسات الشهادات والضوابط المتعلقة بخدمات سلطة التصديق للبريد الإلكتروني الآمن S/MIME وبناءً على هذا التقييم ترى الإدارة أنه عند تقديم خدمات سلطة التصديق للبريد الإلكتروني الآمن S/MIME في بغداد العراق اعتباراً من ٢٠٢٤-٠٧-٠٣ فإن سلطة التصديق للشركة العامة للاتصالات والمعلوماتية.

- أفصحت عن ممارسات أعمال إدارة دورة حياة شهادات البريد الإلكتروني الآمن S/MIME في:
 - سياسة الشهادات وبيان ممارسات الشهادات لسلطة التصديق الوطنية للشركة العامة للاتصالات والمعلوماتية العراقية 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 البريد الإلكتروني الآمن S/MIME 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 S/MIME certificates managing by licensed TSPs is established and protected throughout their lifecycles; and
 - S/MIME 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 – S/MIME Certificates v1.0.3.
- الضوابط مصممة بشكل مناسب ووضعت قيد التنفيذ لتوفير مستوى معقول من التأكيد بأن:
- سلامة المفاتيح وشهادات البريد الإلكتروني الآمن S/MIME المدارة من قبل مزودي خدمات التصديق المرخص لهم محفوظة طوال دورة حياتها.
 - معلومات المشترك في شهادات البريد الإلكتروني الآمن S/MIME مصادقة بشكل صحيح وفقاً لأنشطة التسجيل المجرة من قبل مزودي خدمات التصديق المرخص لهم.
- الضوابط مصممة بشكل مناسب ووضعت 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 مفوضة ومنفذة بشكل صحيح للحفاظ على سلامة أنظمة سلطة التصديق وفقاً لمبادئ ومعايير ويب ترست لسلطات التصديق لشهادات البريد الإلكتروني الآمن S/MIME الإصدار ١,٠,٣.

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

علي ياسين داوود

ITPC PMA Head
03-07-2024

رئيس سلطة إدارة التوقيع الإلكتروني
٢٠٢٤-٠٧-٠٣



ITPC

التعديل أ - Amendment A

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