

التقرير السنوي
١٤٣٣-١٤٣٤هـ

2012

Annual Report

المركز الوطني للتصديق الرقمي
National Center for Digital Certification



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

جدول المحتويات

كلمة معالي وزير الإتصالات وتقنية المعلومات	٤
كلمة سعادة المستشار و المشرف العام على المركز	٥
قائمة المصطلحات	٦
رسالتنا , أهدافنا , عملاؤنا	٨
أنشطة المركز الوطني للتصديق الرقمي	٩
عقود المشاريع المعتمدة (عقود أو تعاميد)	١١
الإنجازات	١٢
قرارات إدارية	٢٥
القوى البشرية والتدريب	٢٦
الهيكل التنظيمي للمركز الوطني للتصديق الرقمي	٢٧
إدارات المركز الوطني للتصديق الرقمي	٢٨
الخاتمة	٢٩

كلمة معالي وزير الإتصالات وتقنية المعلومات



يعاني المتعاملون إلكترونياً من الآثار السلبية الناتجة عن عدم التيقن من هوية الأطراف المتعاملة وصحة المعلومات المتبادلة ودقتها، وعدم وصول طرف آخر إليها أثناء انتقالها أو الاطلاع عليها أو العبث بها، لذا حرصت وزارة الاتصالات وتقنية المعلومات على معالجة هذا الجانب الحيوي والمهم في التعاملات الإلكترونية، وذلك من خلال إنشاء المركز الوطني للتصديق الرقمي الذي يُمكن المتعاملين من التوقيع رقمياً، ويوفر بيئة الكترونية آمنة ذات موثوقية عالية تضمن أمن وسلامة التعامل الذي يتم من خلالها.

وقد حقق المركز في هذا الجانب نتائج متميزة، إذ أصدر أكثر من 339 شهادة تصديق رقمي عن طريق مقدمي خدمات التصديق الحكومي، وطرح عدداً من الخدمات الإلكترونية المبنية على البنية التحتية للمفاتيح العامة، إلى جانب تنفيذ معظم متطلبات الحصول على الاعتراف الدولي بالمركز. ولعرض هذه الإنجازات بشيء من التفصيل، يسرني أن أقدم التقرير السنوي للمركز الوطني للتصديق الرقمي للعام المالي 1433هـ / 1434هـ (2012 م).

وبهذه المناسبة أؤكد أن هذه الإنجازات ما كانت لتتحقق لولا ما قدمته الحكومة الرشيدة من دعم غير محدود بقيادة خادم الحرمين الشريفين وسمو ولي عهده الأمين، مما كان له أبلغ الأثر في تطوير أعمال المركز عاماً بعد عام. كما أجدها فرصة مواتية لتقديم الشكر والتقدير لإدارة المركز وجميع العاملين فيه على ما يبذلونه من جهود متميزة.

والله الموفق،،،

وزير الإتصالات وتقنية المعلومات

م. محمد جميل بن أحمد ملا

كلمة سعادة المستشار و المشرف العام على المركز



يسعدني أن أقدم التقرير السنوي للمركز الوطني للتصديق الرقمي عن العام المالي ١٤٣٣/١٤٣٤هـ (٢٠١٢م)، والذي من خلاله سيتم استعراض نشاطات المركز وإنجازاته خلال العام. تماشياً مع إستراتيجية عمل المركز فقد تم خلال هذا العام ربط خمس جهات حكومية من خلال خدمة "رابط" بزيادة نسبتها ١٥٠٪ عن العام الماضي، وإصدار أكثر من ٣٣٩ شهادة تصديق رقمي، مع ارتفاع في عدد الخدمات الإلكترونية المبنية على منظومة البنية التحتية للمفاتيح العامة بنسبة ١٥٠٪ عن العام الماضي لتصل إلى خمس خدمات إلكترونية من خلال خدمة "تكامل" واعتماد أول وحدة تخزين آمنة لشهادة التصديق الرقمي من خلال خدمة "جاهز" وشراء عدد ٥٠٠٠ وحدة تخزين لدعم الجهات الحكومية وتشجيعها على استخدام الشهادات الرقمية.

كما تم عقد ثمان ورش عمل بزيادة قدرها ٨٠٠٪ عن العام الماضي من خلال خدمة "تدريب" وإنجاز ما نسبته ٩٠٪ من مشاريع برنامج الحصول على شهادة التوافق مع المعيارين (WebTrust for Certification Authorities و ISO٢٧٠٠١) والقيام بعدد من المبادرات مثل مبادرة حلول الموثوقية الرقمية للبنية التحتية للمفاتيح العامة واستراتيجية أمن المعلومات في المملكة العربية السعودية والتوقيع على اتفاقيتي تعاون مع المركز الوطني الإرشادي لأمن المعلومات (CERT) في هيئة الاتصالات وتقنية المعلومات و برنامج التعاملات الإلكترونية الحكومية (يسر) وتفعيل ودعم كافة قنوات الاتصال الممكنة بشكل عام والقنوات الإلكترونية بشكل خاص من خلال اعتماد مشروع تطوير ودعم وإدارة وتشغيل البوابة الإلكترونية للمركز الوطني للتصديق الرقمي.

ختاماً، لا يسعني إلا أن أتقدم بجزيل الشكر وعظيم الإمتنان لمعالي وزير الاتصالات وتقنية المعلومات على دعمه المتواصل للمركز الوطني للتصديق الرقمي وغيره من برامج الوزارة، كما أتقدم بجزيل الشكر لجميع منسوبي المركز الوطني للتصديق الرقمي على جهودهم الطيبة ونشاطهم الدؤوب في تطوير عمل المركز والسعي نحو تحقيق أهدافه بأفضل السبل، ونتطلع إلى عام جديد وإنجازات كبيرة بإذن الله.

المستشار والمشرف العام
على المركز الوطني للتصديق الرقمي
د. فهد بن عبدالله الحويمان

قائمة المصطلحات

← **المركز الوطني للتصديق الرقمي:** هو الجهة التي تقوم بتقديم منظومة متكاملة لإدارة البنية التحتية للمفاتيح العامة، التي تقوم عليها كافة الأعمال الإلكترونية كالتجارة الإلكترونية والتعاملات الإلكترونية الحكومية، لتمكين المتعاملين من إجراء مختلف العمليات الإلكترونية بموثوقية وسلامة تامة.

← **البنية التحتية للمفاتيح العامة (PKI) (بنية المفاتيح العامة):** مجموعة السياسات والقوانين والأجهزة والبرامج والخدمات، التي تمكن المستخدمين من تبادل المعلومات والمعاملات والمفاتيح والتوقيعات الرقمية، بشكل آمن يتيح للأطراف المختصة التأكد من هوية المرسل والمستقبل.

← **مركز التصديق الجذري:** هو أعلى سلطة تصديق تقع في قمة الهرم في بنية المفاتيح العامة وتعود ملكيته للمركز الوطني للتصديق الرقمي، كما أن الشهادة الخاصة بمركز التصديق الجذري موقعة إلكترونياً بشكل ذاتي.

← **مركز التصديق الحكومي:** هو سلطة تصديق تقع في المستوى الثاني في بنية المفاتيح العامة تحت مركز التصديق الجذري مباشرة وتكون الشهادة الخاصة بمركز التصديق الحكومي موقعة رقمياً من مركز التصديق الجذري، ويقوم بإصدار وتصديق الشهادات الخاصة بموظفي وأعمال القطاع الحكومي.

← **مقدمو خدمات التصديق:** الجهات المرخصة المعتمدة لإثبات هوية المتعاملين، وإصدار الشهادات الرقمية لهم.

← **الشهادة الرقمية:** عبارة عن بطاقة تعريف إلكترونية تحتوي على معلومات عن صاحب البطاقة الشخصية والمفتاح المستخدم لتشفير البيانات الموجهة إلى صاحب الشهادة.

قائمة المصطلحات

- ← **شهادة رقمية لمواقع آمنة SSL:** هي عبارة عن شهادة رقمية صادرة من مركز تصديق تحتوي على اسم النطاق لموقع إلكتروني وتستخدم كمعرف للموقع الإلكتروني كما أنها تحمي المعلومات المتراصة بين الموقع والمستخدمين.
- ← **الإستعلام الآلي عن حالة الشهادة الرقمية (OCSP):** تمكن هذه الخدمة مستخدمي بنية المفاتيح العامة من التحقق الآلي من صلاحية الشهادات الرقمية.
- ← **التوقيع الرقمي:** توقيع رقمي يستخدم لعدة أغراض، منها إثبات الهوية في التعاملات الإلكترونية والقيام مقام التوقيع اليدوي التقليدي، ويعتمد على التشفير والبنية التحتية للمفاتيح العامة.
- ← **التعاملات الإلكترونية الحكومية (الحكومة الإلكترونية):** الاستخدام التكاملي الفعال لجميع تقنيات المعلومات والاتصالات، لتسهيل العمليات بين القطاعات الحكومية (حكومية - حكومية "G2G") وتلك التي تربطها بالمواطنين (حكومية - مواطن "G2C") وقطاعات الأعمال (حكومية - أعمال "G2B").
- ← **الخدمات الإلكترونية:** الخدمات المقدمة إلكترونياً عبر وسائل الاتصالات باستخدام تقنية المعلومات.
- ← **البوابة (Portal):** موقع على شبكة الإنترنت يشكل نقطة البداية للاتصال بين زوار الموقع والجهات المختلفة، وقد جاء اسم البوابة من وظيفتها كباب مفتوح يُطل منه على عالم المعلومات والفعاليات الأخرى التي توفرها الجهات ومواقع الإنترنت، وتتميز البوابة عن بقية مواقع شبكة الإنترنت الأخرى بدرجة عالية من التنظيم وجودة المحتوى.

رسالتنا

تحقيق مستوى عال من الثقة في التعاملات الإلكترونية الحكومية والتجارية والفردية في المملكة العربية السعودية من خلال توظيف التقنيات الأمنية المناسبة والسياسات والإجراءات المتطورة.

أهدافنا

- ← تنفيذ وتشغيل وتطوير وإتاحة عدد من الوسائل الخاصة بأمن المعلومات وتوظيفها لتحقيق أهداف البنية التحتية للمفاتيح العامة.
- ← تحقيق سلامة المعلومات من العبث والتغيير والحفاظ على سريتها.
- ← تفعيل خدمات التوقيع الرقمي بواسطة الشهادة الرقمية.

عملاؤنا

- ← تنفيذ وتشغيل وتطوير وإتاحة عدد من الوسائل الخاصة بأمن المعلومات وتوظيفها لتحقيق أهداف البنية التحتية للمفاتيح العامة.
- ← تحقيق سلامة المعلومات من العبث والتغيير والحفاظ على سريتها.
- ← تفعيل خدمات التوقيع الرقمي بواسطة الشهادة الرقمية.

أنشطة المركز الوطني للتصديق الرقمي

← توفير منظومة متكاملة لإدارة البنية التحتية للمفاتيح العامة.

← تشغيل الأجهزة وصيانتها والبرمجيات الخاصة بالبنية التحتية للمفاتيح العامة.

← إصدار الشهادات الرقمية الخاصة بمقدمي خدمات التصديق، وتحديد مدة تلك الشهادات وصلاحياتها،

وتنفيذ المهمات الإجرائية الخاصة بالشهادات.

← نشر قائمة مقدمي خدمات التصديق المرخص لهم والعمل على تحديثها باستمرار.

← إعداد معايير ومتطلبات البنية التحتية للمفاتيح العامة، والتنسيق في ذلك مع الجهات المعنية.

← التنسيق مع هيئة الإتصالات وتقنية المعلومات بشأن الترخيص للجهات التي ترغب في تقديم خدمات

التصديق الرقمي.

← تقديم الدعم الفني للهيئة فيما يخص إشرافها على مقدمي خدمات التصديق المرخص لهم.

← إشعار الهيئة بأي مخالفات تتعلق بتراخيص مقدمي خدمات الترخيص.

أنشطة المركز الوطني للتصديق الرقمي

تشتمل خطة تنفيذ مشروع إنشاء المركز الوطني للتصديق الرقمي على ثلاث مراحل رئيسية، كما يلي:

← **المرحلة الأولى:** تتضمن بناء مقر المركز والضوابط الأمنية المصاحبة له، وتم تنفيذ هذه المرحلة في عام ٢٠٠٧-٢٠٠٨م، من خلال مشروع "إنشاء وتجهيز المركز الوطني للتصديق الرقمي".

← **المرحلة الثانية:** تتضمن هذه المرحلة قسمين رئيسيين أولهما مرحلة إنهاء أعمال التوريد والتركيب والربط والتطبيق لأجهزة وأنظمة وخدمات البنية التحتية للمفاتيح العامة، وقد تم الانتهاء منها نهاية عام ٢٠٠٨م، والقسم الثاني يشمل مرحلة التشغيل الفعلي والصيانة والدعم الفني للمركز لمدة سنتين والتي ابتدأت مباشرة مع نهاية أعمال التوريد والتركيب، وتم تنفيذ كامل هذه المرحلة من خلال عقد مشروع "توريد وتركيب وتشغيل وصيانة البنية التحتية للمفاتيح العامة"، وقد تم الإنتهاء منه منتصف عام ٢٠١٠م.

← **المرحلة الثالثة:** تتضمن هذه المرحلة تنفيذ ما بقي من عناصر البنية التحتية ومتطلبات خدمات التصديق الرقمية للجهات الحكومية وغير الحكومية، وإنجاز مهام تطويرية أخرى ونشر الاستخدام وتعميمه على المستوى الوطني.

عقود المشاريع المعتمدة (عقود أو تعاميد)

- ← تطوير حلول الموثوقية الرقمية للبنية التحتية للمفاتيح العامة.
- ← تطوير وتشغيل وصيانة البوابتين الالكترونيتين الداخلية والخارجية للمركز الوطني للتصديق الرقمي.
- ← توريد عدد (٥٠٠٠) وحدة تخزين آمنة للمركز الوطني للتصديق الرقمي.
- ← طباعة عدد من المستلزمات المكتبية بالشعار الجديد للمركز الوطني للتصديق الرقمي.

الإنجازات



الإنجازات

خمسة جهات حكومية تصدر أكثر من ٣٣٩ شهادة تصديق رقمي

تهدف خدمة "رابط" إلى ربط الجهات الحكومية بالمركز الوطني للتصديق الرقمي وتخويلها بإصدار وإدارة إحتياجها من شهادات التصديق الرقمي من خلال حصولها على مراكز تسجيل خاصة بها، حيث ارتفع عدد الجهات الحكومية التي تم ربطها إلى خمسة جهات حكومية بزيادة نسبتها ١٥٠٪ عن العام الماضي، وقد أصدرت هذه الجهات أكثر من ٣٣٩ شهادة تصديق رقمي، والعمل جار حالياً لربط عدد من الجهات الحكومية الأخرى.

خمسة خدمات إلكترونية مبنية على منظومة البنية التحتية للمفاتيح العامة

تهدف خدمة "تكامل" إلى تقديم الخدمات الاستشارية الفنية اللازمة للجهات الحكومية ومطوري الخدمات الإلكترونية وذلك لمساعدتهم على تطوير الحلول والتطبيقات المبنية على منظومة البنية التحتية للمفاتيح العامة حيث ارتفع عدد الخدمات الإلكترونية المبنية على منظومة البنية التحتية للمفاتيح العامة بنسبة ١٥٠٪ عن العام الماضي لتصل إلى خمس خدمات إلكترونية، تشمل خدمة أوامر الدفع بالتعاون مع وزارة المالية ووزارة الاتصالات وتقنية المعلومات وخدمة البريد الإلكتروني الآمن وخدمة التوقيع على الوثائق بإستخدام مايكروسوفت أوفيس وبرامج أدوبي، كذلك برنامج سماك المحاسبي (SMACC) بالتعاون مع شركة بحر العرب لأنظمة المعلومات، إضافة إلى نظام تخطيط موارد المؤسسات (موارد) من شركة أوراكل بالتعاون مع وزارة الاتصالات وتقنية المعلومات، كما أن العمل جارٍ حالياً على عدد من الخدمات الإلكترونية الأخرى.

إعتماد أول وحدة تخزين آمنة لشهادة التصديق الرقمي

تهدف خدمة "جاهز" إلى إجراء الاختبارات اللازمة على الأجهزة الأمنية (USB Tokens) التي تتقدم بها الشركات المصنعة للمركز للتأكد من جاهزيتها وتحقيقها لمعدلات أمنية عالية المستوى ومن ثم تأهيلها ليتم استخدامها في المملكة العربية السعودية بشكل موثوق، حيث تم تأهيل المنتج (SafeNet iKey4000USB Token) من شركة "سيف نت" العالمية.

وفي نفس السياق وبهدف تطوير أجهزة أمنية وطنية مصنعة محليا تمهيدا لإحلالها بدلا من الأجهزة الأجنبية مستقبلاً، تم البدء في مشروع (عماد-٢) الذي يهدف إلى تطوير جهاز وطني (National Hardware Security Token) بالتعاون مع مدينة الملك عبد العزيز للعلوم والتقنية.

الإجازات

ثمان ورش عمل

تهدف خدمة "تدريب" إلى معالجة قلة الوعي لدى الأفراد والجهات حول منظومة البنية التحتية للمفاتيح العامة وأهميتها ودورها من خلال تقديم عدد من حصص الوعي العام وعقد الندوات والمؤتمرات وورش العمل حيث تم عقد ثماني ورش عمل بزيادة قدرها ٨٠٠٪ عن العام الماضي وذلك بالتعاون مع مركز التميز لأمن المعلومات، تفعيلاً للإتفاقية المبرمة مسبقاً بين جامعة الملك سعود ووزارة الإتصالات وتقنية المعلومات في هذا الشأن حيث إستفاد من هذه الدورات عدد من الجهات في القطاع الحكومي والخاص.

الإجازات

شراء ٥٠٠٠ وحدة تخزين آمنة لشهادة التصديق الرقمي لدعم وتشجيع الجهات الحكومية

رغبة من المركز في نشر استخدام شهادة التصديق الرقمي لدى الجهات الحكومية، ولمساعدة الجهات الحكومية على تقديم خدمات التصديق الرقمي بشكل سريع وتحفيزها للإستفادة من خدمة "رابط" والإنضمام كمقدم خدمات تصديق حكومي، فقد تم تأمين عدد خمسة آلاف وحدة تخزين آمنة لشهادات التصديق الرقمي والتي تم تأهيلها واعتمادها من خلال خدمة "جاهز"، وذلك لمنحها للجهات المستفيدة من خدمة "رابط".

برنامج الحصول على شهادة التوافق مع المعيارين (ISO 27001 و WebTrust for Certification Authorities)

إدراكاً من المركز الوطني للتصديق الرقمي لأهمية توفير أكبر قدر من الحماية للمعلومات ونيل الشهادات الرقمية التي يصدرها المركز للاعتراف الدولي من قبل مصنعي البرامج وأنظمة التشغيل، قام المركز بالعمل على الحصول على شهادة التوافق مع المعيارين (ISO 27001 و WebTrust for Certification Authorities) حيث تمثل هذه المعايير دلالة على التزام المركز بحماية أمن المعلومات، فتم اعتماد برنامج متكامل بهدف توفير، وتطبيق، وتشغيل، ومراقبة، ومراجعة، وإدامة، وتطوير نظام لإدارة أمن معلومات "ISMS"، بما يراعي المخاطر الكلية للتعاملات في المركز. كما إن هذا البرنامج يسعى إلى تقديم خدمات ذات جودة عالية ووفق أفضل الممارسات والسياسات واللوائح العالمية بحيث يقوم بالتأكد من توافق عمليات تشغيل البنية التحتية للمفاتيح العامة مع سياسة الشهادة الرقمية وإجراءات التصديق الرقمي، بالإضافة إلى السياسات والإجراءات التشغيلية.

برنامج الحصول على شهادة التوافق مع المعيارين (ISO 27001 و WebTrust for Certification Authorities)

تم إنجاز مانسبته ٩٠٪ من مشاريع البرنامج هذا العام، حيث تم الإنتهاء من ترقية خوارزمية التشفير المستخدمة في المفاتيح العامة والخاصة في مركزي التصديق الجذري والحكومي من خوارزمية "SHA1" إلى "SHA2" وتم الإنتهاء من إعداد مركز بيانات رديف لأغراض ضمان الاستمرارية في العمل في حال الكوارث وتوريد وتركيب قاطع كهربائي آلي في مركز البيانات الأساسي ليقوم بتحويل مصدر الطاقة الكهربائية الرئيس إلى مولد الكهرباء الإحتياطي بشكل آلي في حال انقطاعها وتوفير الضمان والصيانة والدعم الفني لمدة ثلاث سنوات.

كما تم تطبيق أجهزة وتقنيات تحليل أمنية لتقييم الوضع الأمني الحالي للمركز بشكل دوري وتحديد مواطن الثغرات الأمنية المحتملة التي قد تسبب خطراً على العمليات والمعلومات المتعلقة ببنية المفاتيح العامة وتم العمل على إعداد ومراجعة أكثر من ١٦ سياسة أمنية للمركز والقيام بأعمال المراجعة والتدقيق الداخلي للمركز وذلك للتأكد من الالتزام التام وتوافق الاجراءات المطبقة مع كافة السياسات واللوائح المعتمدة من الإدارة العليا للمركز وقياس توافق وجاهزية المركز مع متطلبات CA/Browser Forum.

حلول الموثوقية الرقمية للبنية التحتية للمفاتيح العامة

إن قلة التطبيقات التي تستخدم منظومة البنية التحتية للمفاتيح العامة تعتبر من أهم التحديات التي تواجه المركز، لذا بادر المركز بدراسة تلك المشكلة والعمل على إيجاد حلول عملية لها وذلك من خلال الإستعانة بأحد بيوت الخبرة للحصول على خدمات استشارية لغرض إعداد آلية مناسبة لتطوير خدمات الموثوقية الرقمية والتحقق من الهوية وتعزيز استخدام التواقيع الرقمية من خلال حلول وتطبيقات متكاملة يتبنى المركز تنفيذها بشكل مركزي.

وقد تم إنجاز المرحلتين الأولى والثانية من المشروع وذلك بعمل دراسة مقارنة دولية للتجارب المطبقة في حلول وتطبيقات الموثوقية الرقمية مثل التوقيع الرقمي والتحقق من الهوية (كحلول مركزية للموثوقية)، شاملة كافة تفاصيل الخدمات المقدمة وطرق تنفيذها والتطبيقات واستخداماتها وكذلك القواعد والشروط المطبقة حيال ذلك في كل دولة تشملها الدراسة ودراسة وتحليل تطبيقات الأعمال المستخدمة لدى القطاع العام والخاص في المملكة وتقييم مدى احتياجها لخدمات التوقيع الرقمي والتحقق من الهوية من خلال حلول مركزية أو بوابة مشتركة.

وقد تضمن ذلك القيام بعمل مسح ميداني ونموذج استبيان وتحليل وتلخيص النتائج وإعداد قائمة بالتطبيقات الممكن تقديمها ضمن حلول الموثوقية المقترحة مع تقديم وصف عام وتحليل فني عام لكل تطبيق وتحديد متطلبات القوى العاملة والخبرات المطلوبة لتنفيذ الحلول المقترحة. وشمل ذلك تحديد المؤهلات والخبرة وعدد الموظفين المطلوب وإعداد كافة المتطلبات الفنية لتنفيذ الحلول المقترحة، بما في ذلك البرامج والأجهزة ومتطلبات التطبيقات والمتطلبات الأمنية والمتطلبات الخاصة ببنية المفاتيح العامة وإعداد كراسة مناسبة لطلب معلومات (RFI) عن الحلول المقترحة، لتوجيهها للشركات وبيوت الخبرة ذوات العلاقة، وتحليل كافة الردود وتقييمها وتضمين نتائجها في خطة تنفيذ المشروع والتكلفة المتوقعة.

البوابتان الإلكترونية الداخلية والخارجية للمركز الوطني للتصديق الرقمي

تنفيذاً لإستراتيجية المركز في الإتصال والتي تنص على أهمية تفعيل ودعم كافة قنوات الإتصال الممكنة بشكل عام والقنوات الإلكترونية بشكل خاص، فقد تم اعتماد مشروع تطوير ودعم وإدارة وتشغيل البوابة الإلكترونية للمركز الوطني للتصديق الرقمي بهدف تطوير قنوات إلكترونية يتم من خلالها التواصل مع العملاء وتقديم عدد من الخدمات إلكترونياً حيث تم توقيع العقد مع إحدى الشركات المتخصصة.



إستراتيجية أمن المعلومات في المملكة العربية السعودية

نظراً لأهمية أمن المعلومات في المجتمع المعلوماتي، واستجابة لقرار مجلس الوزراء رقم (٨٢) وتاريخ ١٤٣١/٣/٢٢هـ القاضي بالموافقة على توصيات مؤتمر تقنية المعلومات والأمن الوطني المنعقد في الرياض خلال الفترة ٢١-٢٤/١١/١٤٢٨هـ والمتضمن تكليف وزارة الاتصالات وتقنية المعلومات بإعداد استراتيجية وطنية لأمن المعلومات، كلف معالي وزير الاتصالات وتقنية المعلومات المركز الوطني للتصديق الرقمي بتطوير استراتيجية وطنية لأمن المعلومات إيماناً منه بأهمية دور المركز في ذلك وبما يتميز به من خبرات وكوادر مؤهلة على مستوى عالٍ من الكفاءة في أمن المعلومات وقد تم الإنتهاء من إعداد مسودة الإستراتيجية وطلب مرئيات العموم حولها حيث من المتوقع ان يتم إصدار النسخة النهائية في العام الحالي إن شاء الله.

المشاركة في معرضي جايتكس الرياض ٢٠١٢ م، والإتصالات الدولي (ITU) في دبي

تحت رعاية وزارة الاتصالات وتقنية المعلومات شارك المركز بجناح قَدَم من خلاله عدد من العروض في معرض جايتكس الرياض ٢٠١٢، ومعرض الإتصالات الدولي (ITU) في دبي.



إتفاقية تعاون مع المركز الوطني الإرشادي لأمن المعلومات (CERT) في هيئة الإتصالات وتقنية المعلومات و برنامج المعاملات الإلكترونية الحكومية (يسر)

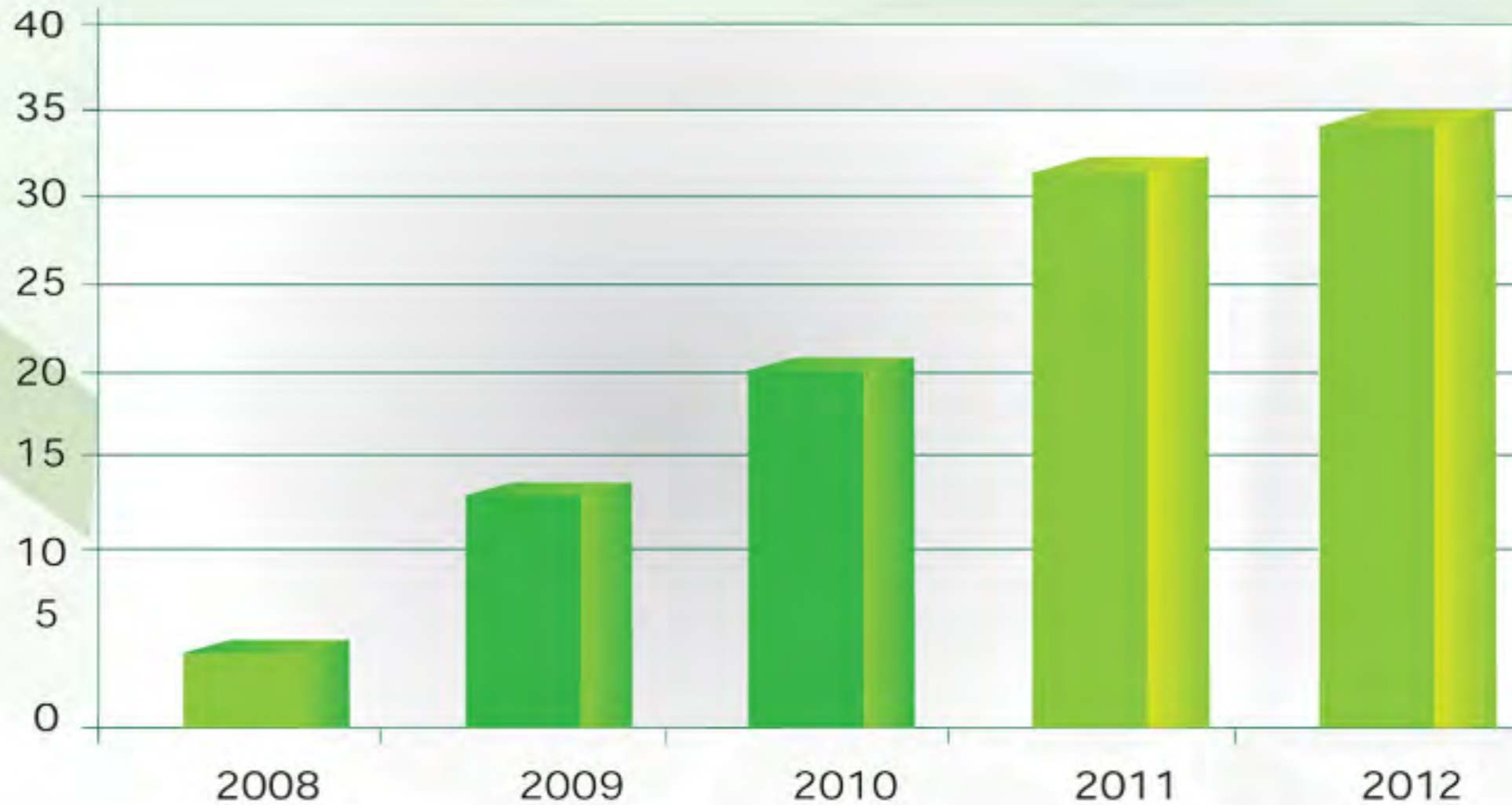
إيماناً بأهمية التعاون ومبدأ الشراكة الإستراتيجية مع الجهات ذات الصلة لتحقيق أهداف المركز تم التوقيع على إتفاقتي تعاون، الأولى مع المركز الوطني الإرشادي لأمن المعلومات (CERT) في هيئة الإتصالات وتقنية المعلومات وذلك للاستفادة من الخدمات التي يقدمها للجهات الحكومية كبرامج التوعية والسياسات الأمنية والخدمات الفنية والإنذارات الأمنية. أما الإتفاقية الثانية فتتمت مع برنامج المعاملات الإلكترونية الحكومية (يسر) من أجل نشر استخدام شهادات التصديق الرقمي في المعاملات الإلكترونية المقدمة من قبل الجهات الحكومية والتي يقوم برنامج يسر بتقديم خدمات استشارية لها في مجال تطوير وتمكين استراتيجية المعاملات الإلكترونية وذلك من خلال تقييم احتياجات هذه الجهات للشهادات الرقمية وتحديد أفضل الأساليب والطرق لتفعيل استخدامها في الخدمات الإلكترونية المقدمة ضمن جدول زمني وحسب الأولويات.

قرارات إدارية

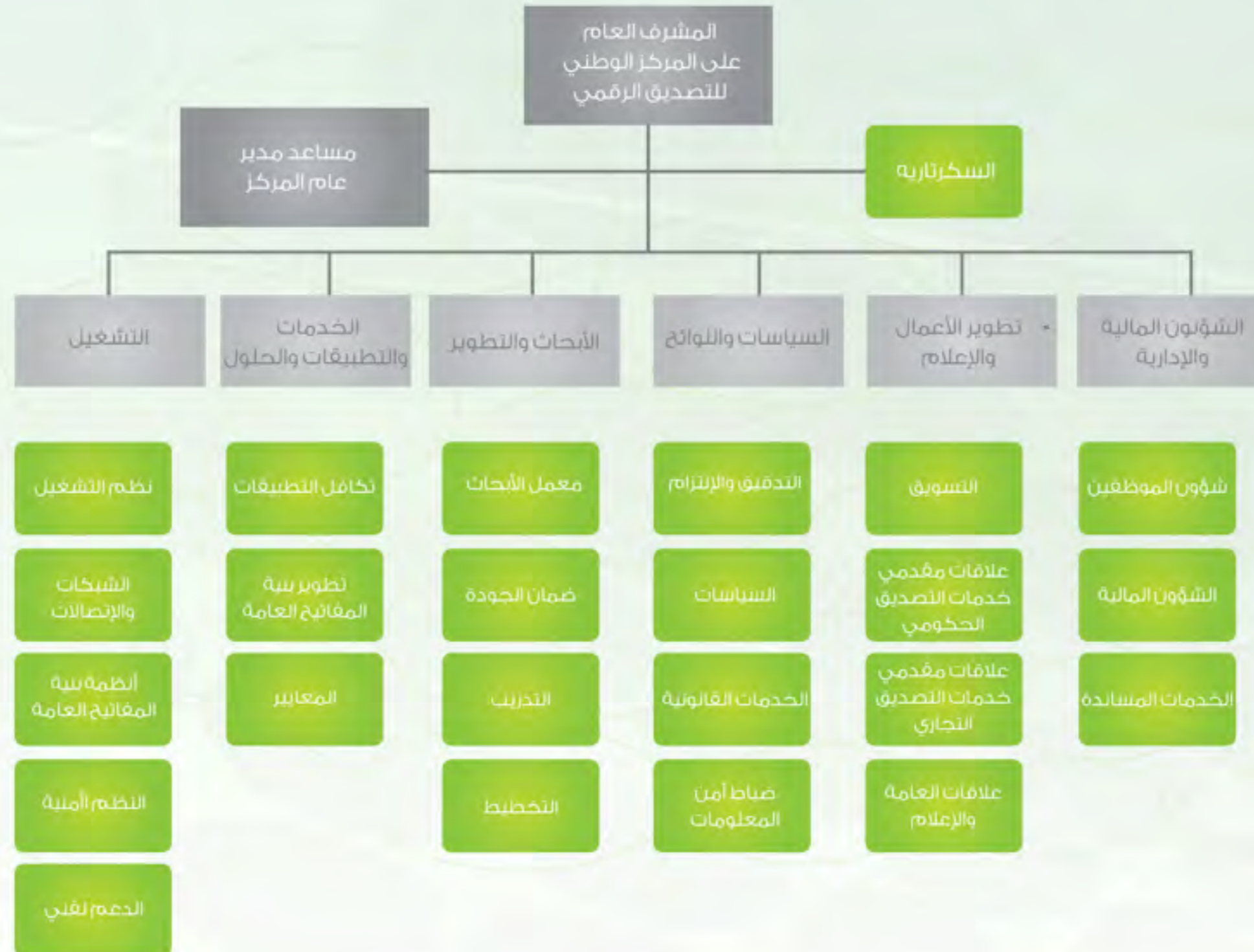
- ← قرار رقم ٤/١٠٩٧٣ وبتاريخ ١٤٣٣/١٢/٢٩ هـ القاضي بتمديد تكليف بعض موظفي المركز.
- ← قرار رقم ٤/٦٤٢٠ وبتاريخ ١٤٣٣/٦/٣٠ هـ القاضي بتعيين مسؤول أمني بمركز خدمات التصديق الخاص بالمركز الوطني للتصديق الرقمي.
- ← قرار رقم ٤/٧٠٣ وبتاريخ ١٤٣٤/١/١٩ هـ القاضي بتشكيل فريق عمل لتنفيذ مشروع تطوير وتشغيل وصيانة البوابتين الداخلية والخارجية للمركز الوطني للتصديق الرقمي.
- ← قرار رقم ٤/٧٤٤٧ وبتاريخ ١٤٣٣/٧/٢٩ هـ القاضي بتشكيل فريق عمل لتنفيذ مشروع تطوير حلول الموثوقية للبنية التحتية للمفاتيح العامة.

القوى البشرية والتدريب

تمكن المركز الوطني للتصديق الرقمي من استقطاب وتوظيف الكفاءات السعودية المؤهلة في مختلف المهن والتخصصات ذات العلاقة بطبيعة العمل في المركز ليصبح عدد موظفي المركز خمسة وثلاثون موظفاً، وقد بلغ عدد البرامج التدريبية التي تم تنفيذها للموظفين السعوديين في الداخل والخارج خلال العام المالي ١٤٣٣/١٤٣٤ هـ تسعة عشر برنامجاً تدريبياً.



الهيكل التنظيمي للمركز الوطني للتصديق الرقمي



إدارات المركز الوطني للتصديق الرقمي

- ← **إدارة الشؤون المالية والإدارية:** وتقوم بإدارة العمليات المالية والمحاسبية والإجراءات الخاصة بشؤون الموظفين وعمليات التوظيف والخدمات التابعة لها وفقاً للأنظمة واللوائح المعمول بها، وتشمل الأقسام: شؤون الموظفين، الشؤون المالية، الخدمات المساندة، وحالياً يتولى مهام هذه الإدارة منسق للشؤون المالية والإدارية.
- ← **إدارة تطوير الأعمال والإعلام:** وتقوم بالتسويق لمنتجات وخدمات المركز، وذلك من خلال التواصل مع المستفيدين من هذه الخدمات والمنتجات، وبناء شراكة استراتيجية مع عدد من الجهات الحكومية والقطاع الخاص والتعامل مع وسائل الإعلام المختلفة، وتشمل الأقسام: التسويق، علاقات مقدمي خدمات التصديق الحكومي، علاقات مقدمي خدمات التصديق التجاري، العلاقات العامة والإعلام.
- ← **إدارة السياسات واللوائح:** وتقوم بإعداد السياسات والإجراءات واللوائح الخاصة بعمل المركز أو المتعلقة بالخدمات التي يقدمها المركز، كما تقوم بضمان الالتزام بهذه السياسات والإجراءات واللوائح عبر عمليات التدقيق، وتشمل الأقسام: التدقيق والالتزام، السياسات، الخدمات القانونية، ضابط أمن المعلومات.
- ← **إدارة الأبحاث والتطوير:** وتقوم بالأبحاث المتعلقة بتطوير تقنية المفاتيح العامة والتشفير، كما تقوم بعمليات التدريب وضمان الجودة لخدمات ومنتجات المركز، وتشمل الأقسام: معمل الأبحاث، ضمان الجودة، التدريب، التخطيط.
- ← **إدارة الخدمات والتطبيقات والحلول:** وتقوم بتطوير وصيانة التطبيقات والبرامج الخاصة بعمل المركز أو المتعلقة بالخدمات المعتمدة على بنية المفاتيح العامة، كما تقوم بدراسة وتطبيق أفضل الحلول لربط وتكامل التطبيقات والأجهزة المعتمدة على بنية المفاتيح العامة، وتشمل الأقسام: تكامل التطبيقات، تطوير بنية المفاتيح العامة، المعايير.
- ← **إدارة التشغيل:** وتقوم بعمليات التشغيل لمركز بيانات المركز ومركز الخدمات المشتركة عبر إدارة الأنظمة والأجهزة الخاصة بتقنية المفاتيح العامة وما يتعلق بها من أنظمة التشغيل والشبكات والأنظمة الأمنية والدعم الفني، وتشمل الأقسام: نظم التشغيل، الشبكات والاتصالات، أنظمة بنية المفاتيح العامة، النظم الأمنية، الدعم الفني.

الخاتمة

يشمل هذا التقرير أهم إنجازات المركز الوطني للتصديق الرقمي خلال العام المالي ١٤٣٣/١٤٣٤هـ (٢٠١٢ م)، وسيتم في هذا العام بإذن الله الاستمرار في متابعة تنفيذ مشاريع المركز الوطني للتصديق الرقمي وتطويره، والمشاركة في الفعاليات المحلية والدولية ذات العلاقة.