

التقرير السنوي  
١٤٣٥-١٤٣٥هـ

2013

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	٢٢
القوى البشرية والتدريب	٢٣
الهيكل التنظيمي للمركز الوطني للتصديق الرقمي	٢٤
إدارات المركز الوطني للتصديق الرقمي	٢٥
الخاتمة	٢٦

## كلمة معالي وزير الإتصالات وتقنية المعلومات



يشكل أمن المعلومات أساساً مهماً في التعاملات الإلكترونية وهو ما تعمل عليه وزارة الاتصالات وتقنية المعلومات، ممثلة في المركز الوطني للتصديق الرقمي للإسهام في رفع مستوى السلامة والموثوقية في التعاملات الإلكترونية. وقد تضمن التقرير بشائر بكثير من المنجزات؛ منها ارتفاع عدد الجهات الحكومية التي تقدم خدمات التصديق الحكومي. وكذلك حصول المركز على شهادة التوافق مع المعيار العالمي المعروفة بـ (Web Trust for Certification Authorities) وغيرها، بل والسعي إلى تطوير أجهزة أمنية وطنية مصنعة محلياً تمهيداً لإحلالها مكان الأجهزة الأجنبية في المستقبل ... وغيرها كثير من نتائج خيرة يزفها التقرير السنوي للمركز عن العام المالي ١٤٣٤/١٤٣٥ هـ (٢٠١٣م). وقد تم من خلال هذا التقرير استعراض نشاطات المركز، وما حققه خلال العام. ونتطلع إلى مزيد من الإنجازات لتحقيق الأهداف المرجوة من إنشاء المركز في ظل الدعم المستمر من قبل الدولة؛ للرقى بمستوى الخدمات الحكومية الإلكترونية. وأجدها فرصة مواتية لتقديم الشكر والتقدير لإدارة المركز، وجميع العاملين فيه على ما يبذلونه من جهود جعلت إنجازات المركز تتواصل عاماً بعد عام.

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 ١٤٣٤/١٤٣٥ هـ (٢٠١٣م)، والذي من خلاله سيتم استعراض نشاطات المركز وإنجازاته خلال العام.

تماشياً مع إستراتيجية عمل المركز فقد تم خلال هذا العام ربط ست جهات حكومية من خلال خدمة "رابط"، مع ارتفاع في عدد الخدمات الإلكترونية المعتمدة على منظومة البنية التحتية للمفاتيح العامة. وبالنسبة لخدمة "تكامل"، فقد حقق المركز شهادة التوافق مع المعيار العالمي WebTrust for Certification Authorities وذلك بعد اجتياز مرحلة التدقيق والمراجعة من قبل فريق خبراء من جهة عالمية معتمدة للحصول على الشهادة. كما أنه قد تم انضمام المركز لقائمة مركز الاتصال الوطني "آمر"، الذي يقدم خدمة الرد على استفسارات الجمهور و

والمستفيدين من التعاملات الإلكترونية الحكومية وتقديم الدعم وتوفير المعلومات عن الخدمات والتعاملات الإلكترونية المقدمة من الجهات الحكومية للمستفيدين. خلال العام المنصرم، تم كذلك إطلاق مبادرة خدمة "البريد الإلكتروني الآمن"، التي تمكن المستخدمين من إضافة التوقيع الإلكتروني إلى المراسلات البريدية، وإضافة آلية التشفير إلى المحتوى. وقد قام المركز بالتنسيق مع بعض الجهات الحكومية مثل برنامج "يسر" والبريد السعودي وهيئة الاتصالات وتقنية المعلومات وهيئة السوق المالية ومؤسسة النقد العربي السعودي لتمكين تلك الجهات من الاستفادة من خدمة التحقق من الهوية وسلامة المحتوى في مراسلاتها عبر البريد الإلكتروني.

ختاماً، لا يسعني إلا أن أتقدم بجزيل الشكر وعظيم الإمتنان لمعالي وزير الإتصالات 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 المتراصلة 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

- ← مقدمو الخدمات الإلكترونية من جهات حكومية وشركات ممن يرغبون في تطوير خدماتهم الإلكترونية الداخلية والخارجية.
- ← مقدمو خدمات التصديق الرقمي الذين يصدرون الشهادات الرقمية لعملائهم.
- ← مستخدمو الخدمات الإلكترونية من جهات حكومية وشركات.



## 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)

- ← مشروع الضمان والصيانة لأنظمة وبرامج ورخص مركز بيانات المركز الوطني للتصديق الرقمي.
- ← البدء بتشغيل وصيانة البوابتين الالكترونيتين الداخلية والخارجية للمركز الوطني للتصديق الرقمي.
- ← مذكرة تفاهم لإنشاء مبنى المركز الوطني للتصديق الرقمي في مجمع تقنية المعلومات والاتصالات التابع للمؤسسة العامة للتقاعد.
- ← مشروع الضمان والصيانة للمكونات التقنية لمركز بيانات المركز الوطني للتصديق الرقمي، الذي يشمل أعمال الصيانة الدورية وإصلاح الأعطال المفاجئة وتوريد قطع الغيار اللازمة والمستهلكات المطلوبة.

# الإنجازات

سبع جهات حكومية تنضم كمقدمي خدمات تصديق حكومي

ارتفع عدد الجهات الحكومية التي تم ربطها إلى سبع جهات حكومية بزيادة نسبتها ١٧٥% عن العام الماضي، والعمل جارٍ حالياً لربط عدد من الجهات الحكومية الأخرى، وقد تم ذلك من خلال خدمة "رابط" التي تهدف إلى ربط الجهات الحكومية بالمركز الوطني للتصديق الرقمي وتخويل تلك الجهات بإصدار وإدارة إحتياجها من شهادات التصديق الرقمي من خلال مراكز تسجيل خاصة بها. والجهات الحكومية التي تم ربطها هي التالية:



برنامج الحصول على شهادة التوافق مع المعايير العالمية:

## تحقيق شهادة WebTrust for Certification Authorities

إدراكاً من المركز الوطني للتصديق الرقمي لأهمية توفير أكبر قدر من الحماية للمعلومات ونيل الشهادات الرقمية التي يصدرها المركز على الإعتراف الدولي من قبل مصنعي البرامج وأنظمة التشغيل التي تتعامل بالشهادات الرقمية، فقد حصل المركز على شهادة التوافق مع المعيار العالمي WebTrust for Certification Authorities وذلك بعد اجتياز مرحلة التدقيق والمراجعة من قبل طاقم من الخبراء التابعين لجهة عالمية معتمدة للحصول على هذه الشهادة.

## برنامج الحصول على شهادة التوافق مع المعايير العالمية:

## تنفيذ مشروع التوافق مع معيار (ISO 27001)

بدأ المركز في تنفيذ مشروع التوافق مع المعيار (ISO 27001) لأمن المعلومات من خلال كفاءات داخلية من المختصين في المركز، حيث تمثل هذه المعايير دلالة على التزام المركز بحماية أمن المعلومات والتزامه بالمعايير الدولية. لذا فقد تم اعتماد برنامج متكامل بهدف توفير وتطبيق وتشغيل ومراقبة ومراجعة وإدامة وتطوير نظام لإدارة أمن معلومات "ISMS" يهدف إلى تقديم خدمات ذات جودة وموثوقية عاليتين، وفق أفضل الممارسات والسياسات واللوائح العالمية. ويشمل ذلك التأكد من توافق عمليات تشغيل البنية التحتية للمفاتيح العامة مع سياسة الشهادة الرقمية وإجراءات التصديق الرقمي، بالإضافة إلى السياسات والإجراءات التشغيلية.

تمثل البرمجيات جزءاً مهماً في عملية تحول التعاملات الورقية إلى تعاملات رقمية. لذا فقد قام المركز بتطوير عدد من البرمجيات التي تسهل عملية استخدام التوقيع الرقمي في التعاملات الحكومية، أخذاً في الاعتبار عدداً من العوامل، منها أن تلبية هذه التطبيقات احتياجات الجهات الحكومية، وأن تكون التطبيقات قابلة للتكامل مع الأنظمة القائمة بشكل سلس، وأن يراعى في تصميم الواجهات سهولة الاستخدام لمن ليس لهم خبرة كبيرة في التعامل مع الحاسب الآلي. وتشمل هذه البرمجيات ما يلي:

### التطبيق الموحد للتوقيع على أوامر الدفع:

يستعمل هذا التطبيق من قبل الجهات الحكومية للتوقيع رقمياً على أوامر الدفع الموجهة لوزارة المالية مع إمكانية التأكد من صحة التوقيع.

### التوقيع على مستندات PDF:

تم إعداد تطبيق خاص بتوقيع الملفات من نوع PDF، بحيث تتم حماية المحتوى من التغيير أو الاختلاف عند استعماله على أجهزة مختلفة.

### التوقيع على ملفات من نوع XML:

تم إعداد تطبيق خاص بتوقيع الملفات من نوع XML تستخدم كوسيلة للتواصل بين الأنظمة الحاسوبية المتنوعة.

### خدمة توقيع مستندات PDF على الإنترنت:

تم تنفيذ خدمة موجهة لحاملي التوقيع الرقمي تمكنهم من توقيع ملفات PDF مباشرة من بوابة المركز الوطني للتصديق الرقمي، دون الحاجة لتنصيب برمجيات إضافية على أجهزتهم.

### البوابة الخاصة بالمركز الوطني للتصديق الرقمي:

تم إطلاق بوابة المركز الوطني للتصديق الرقمي التي تحتوي على معلومات عن المركز وخدماته، إلى جانب المعلومات المتعلقة بمراكز التصديق بمستوياتها الجذري والحكومي. ويمكن الوصول للبوابة على الرابط: [www.ncdc.gov.sa](http://www.ncdc.gov.sa)

## إعتماد وحدة تخزين آمنة لشهادات التصديق الرقمي

استمراراً لعملية اختبار وتأهيل حلول أنظمة التشفير والتخزين للشهادات الرقمية (USB Tokens and Smart Cards)، فقد تم من خلال خدمة "جاهز" تأهيل المنتج eToken 5100 من شركة Safenet العالمية، وذلك للتأكد من مطابقتها للمعايير التقنية العالمية.

وفي السياق ذاته، وبهدف تطوير أجهزة أمنية وطنية مصنعة محلياً تمهيداً لإحلالها مكان الأجهزة الأجنبية مستقبلاً، تم الانتهاء من تنفيذ مشروع ( عماد2-) مع مدينة الملك عبد العزيز للعلوم والتقنية، الذي يهدف إلى تطوير جهاز أمني وطني (National Hardware Security Token) والبدء في مراحل الاختبار والتقييم لهذه التقنية بهدف حفظ الشهادة الرقمية بشكل آمن.



## مذكرة تفاهم مع تكنولوجيا المعلومات بجمهورية مصر العربية

تم التوقيع على مذكرة تفاهم للتعاون في مجال البنية التحتية للمفاتيح العامة بين وزارة الاتصالات وتقنية المعلومات ممثلة بالمركز الوطني للتصديق الرقمي ووزارة الاتصالات وتكنولوجيا المعلومات بجمهورية مصر العربية ممثلة بهيئة تنمية صناعة تكنولوجيا المعلومات، حيث تهدف الاتفاقية إلى التعاون المشترك في الربط والتنظيم بين مركزي التصديق الرقمي الجذريين في كلا الدولتين، إضافة إلى تبادل ونقل الخبرات في مجال أمن المعلومات المتعلقة بأنظمة البنية التحتية للمفاتيح العامة (PKI).

## تنفيذ مشروع نظام إدارة استمرارية العمل Business Continuity Management System

قام المركز بتأسيس برنامج لنظام إدارة استمرارية العمل وفق المعيار العالمي BS25999 المسمى حالياً بالمعيار ISO22301، وقد تم تنفيذ كافة الاجراءات واعداد الوثائق اللازمة، كتحليل المخاطر وتحليل التأثيرات وإعداد استراتيجيات استمرارية العمل وخططها، والتوعية الأمنية، وغيرها. كما قام المركز بالمراجعة الدورية لهذه الاجراءات وعمل الاختبارات الدورية اللازمة لتأكد من جاهزية المركز وأنظمتة التشغيلية في حال وجود الأزمات والكوارث الطبيعية.

## مشروع اختبار الاختراقات الأمنية

حرصاً من المركز على التأكد من سلامة الاعدادات الأمنية للأنظمة فإنه يتم بشكل نصف سنوي عمل اختبارات تتعلق بالاختراقات الأمنية للتأكد من عدم وجود ثغرات أمنية يمكن استغلالها لتشكيل مخاطر أمنية وفنية على العمليات والمعلومات المتعلقة ببنية المفاتيح العامة.

## انضمام المركز لخدمة مركز الاتصال الوطني "آمر"

تم انضمام المركز الوطني للتصديق الرقمي لقائمة مركز الاتصال الوطني "آمر"، الذي يقدم خدمة الرد على استفسارات الجمهور والمستفيدين من التعاملات الإلكترونية الحكومية وتقديم الدعم وتوفير المعلومات فيما يتعلق بالخدمات والتعاملات الإلكترونية المقدمة من الجهات الحكومية للمستفيدين.

## مشروع توريد وتركيب أجهزة وأنظمة فنية لمركز البيانات بالمركز الوطني للتصديق الرقمي

تمت ترسية مشروع توريد وتركيب أجهزة وأنظمة فنية، وذلك نظراً لحاجة المركز لتأمين احتياج مراكز البيانات لتوريد وتركيب أنظمة البيئات الافتراضية والنظم الاحترافية المعنية بتطبيق معايير الجودة لبيئات تقنية المعلومات والجدران النارية والشبكات، إضافة إلى نظام النسخ الاحتياطي وأنظمة المراقبة. وقد تم العمل بهذا المشروع بسبب تقادم بعض الأنظمة الحالية ووصولها إلى العمر الافتراضي الذي تتوقف عنده خدمات الصيانة من الشركة المصنعة، أو بسبب ارتفاع تكلفة صيانة بعض الأنظمة والمعدات الفنية الحالية مقارنة بتكلفة توريد أنظمة جديدة مدعومة بالصيانة. وقد تمت ترسية المشروع بناء على التحليل الفني للجنة الفنية المكلفة بذلك على أن يبدأ التنفيذ خلال عام ٢٠١٤ م.

## مشروع تجديد الضمان والصيانة لأنظمة وبرامج ورخص مركز بيانات المركز الوطني للتصديق الرقمي

نظراً لقرب انتهاء صلاحية فترة الضمان والدعم الفني لرخص الاستخدام لكافة مكونات مركز البيانات بتاريخ ٢٠١٤/٣/٣١ م، فقد تمت مراجعة جدول الكميات وتفصيل المكونات الرئيسية لمركز البيانات من أجهزة وأنظمة ورخص للخدمات ومقاسم الشبكة والأجهزة الأمنية الرئيسية وكافة تجهيزات بنية المفاتيح العامة، وتمت مخاطبة الشركات المعنية لدراسة البدائل المتاحة والاعمار الافتراضية للدعم من مقدمي الخدمات، وتم جمع المعلومات الأساسية التي طرحت كمنافسة حكومية مطلع عام ٢٠١٤ م.

## الإجازات

### مشروع تجديد الصيانة لمكونات مركز بيانات المركز الوطني للتصديق الرقمي

تمت مراجعة جداول الكميات وتفصيل المكونات الرئيسية من أجهزة تغذية كهربائية وأنظمة تكييف وأنظمة مكافحة الحريق وأنظمة مراقبة الدخول وغيرها من الأنظمة المساعدة، وقد تم تعميم إحدى الشركات لتقديم عرضها، حيث تنتهي صلاحية فترة الضمان والصيانة لمكونات مركز البيانات بنهاية عام ٢٠١٣م.

### حلول الموثوقية الرقمية للبنية التحتية للمفاتيح العامة

تم طرح وثيقة مشروع "توريد وتركيب وتشغيل وصيانة حلول الموثوقية الرقمية للبنية التحتية للمفاتيح العامة" في منافسة عامة واسقبال العروض من الشركات والمؤسسات المتقدمة للمنافسة، وتم الانتهاء من دراسة العروض المقدمة فنيا ورفع التوصيات إلى لجنة العروض لاختيار الجهة الفائزة بالمنافسة. ويعد ذلك استكمالاً لما قام به المركز في العام السابق، حيث تم إنجاز المرحلتين الأولى والثانية من المشروع وذلك بعمل دراسة مقارنة دولية للتجارب المطبقة في حلول وتطبيقات الموثوقية الرقمية.

## الإنجازات

### البوابتان الإلكترونية الداخلية والخارجية للمركز الوطني للتصديق الرقمي

تنفيذاً لإستراتيجية المركز في الإتصال والتواصل، التي تركز على أهمية تفعيل ودعم كافة قنوات الإتصال الممكنة بشكل عام والقنوات الإلكترونية بشكل خاص، فقد تم تعميم مشروع "تطوير وتشغيل وصيانة البوابتين الداخلية والخارجية للمركز الوطني للتصديق الرقمي" مع شركة باب العالمية، وذلك بناء على تقييم اللجنة الفنية للمشروع، ويجري العمل على المشروع على أن يتم إطلاق البوابتين خلال عام ٢٠١٤.

### مبادرة تقديم خدمة البريد الإلكتروني الآمن

تعزيزاً لإضافة أعلى وسائل الأمان في استخدامات البريد الإلكتروني تم إطلاق مبادرة خدمة "البريد الإلكتروني الآمن"، التي تمكن المستخدمين من إضافة التوقيع الإلكتروني على المراسلات بالإضافة إلى تشفير المحتوى. وقد قام المركز بالتنسيق مع بعض الجهات الحكومية مثل برنامج "يسر"، والبريد السعودي، وهيئة الاتصالات وتقنية المعلومات، وهيئة السوق المالية، ومؤسسة النقد العربي السعودي، وذلك لتمكين تلك الجهات من ضمان التحقق من الهوية وسلامة المحتوى في مراسلاتها عبر البريد الإلكتروني.

## قرارات إدارية

← قرار رقم ٤/١٠٩٧٣ وبتاريخ ١٤٣٣/١٢/٢٩ هـ القاضي بتمديد تكليف بعض موظفي المركز.

← قرار رقم ٤/٦٦٧٨ وبتاريخ ١٤٣٤/١١/٢٣ هـ بشأن تكليف بعض الموظفين بمهام رئاسة الأقسام التابعة لإدارة التشغيل بالمركز.

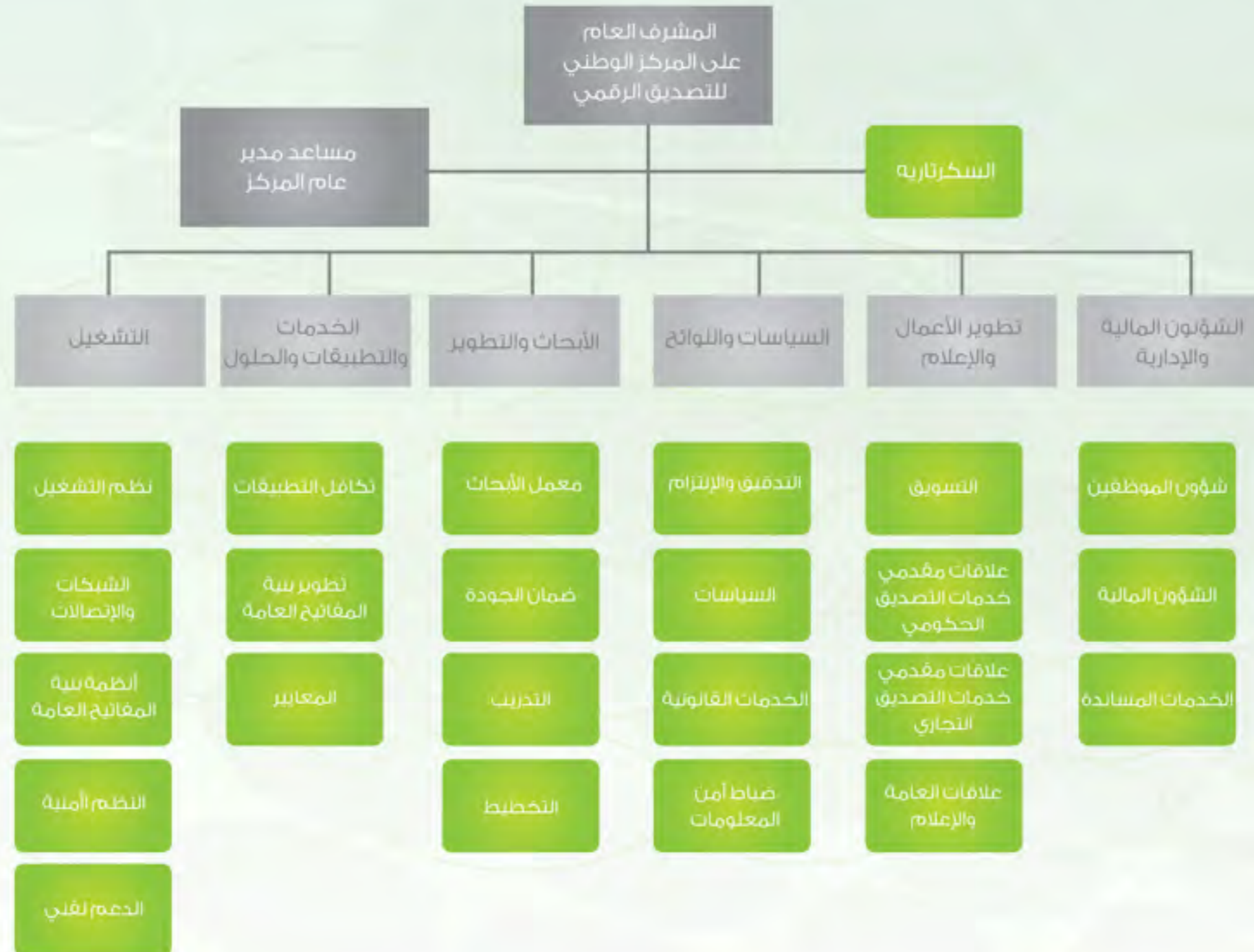
← قرار رقم ٤/٥٦٣٨ وبتاريخ ١٤٣٤/٨/٢٥ هـ بشأن إنهاء تكليف المهندس - باراك باريك من مهمة مدير إدارة الخدمات والتطبيقات والحلول - وتكليف المهندس - وائل عيد بدلاً عنه.

## 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 واحد وثلاثون موظفاً، وقد بلغ عدد البرامج التدريبية التي تم تنفيذها للموظفين السعوديين في الداخل والخارج خلال العام المالي ١٤٣٤/١٤٣٥ هـ ثلاثة عشر برنامجاً تدريبياً كالتالي:

الموقع	اسم البرنامج
الدمام	Junos Security and Unified Threat Management
كوالا لمبور	Nwtwork Security Administorator , Princeto combined Practitoner Program with Exams
دبي	الكفاءة والتنظيم المتميز في إدارة أعمال مكاتب الإدارة العليا والتنفيذية
لندن	Certified information systems Auditor , Certified Informaton Security Manager
بريطانيا	ISACA CISM (certified InfoSecurity Manager) , EC-Conuncil Securtiy Analyst/Lead PenTester
جدة	تنمية المهارات الإدارية والقيادية
دبي	الاستراتيجيات المتقدمة والتميز في تطوير وتنمية الموارد البشرية
دبي	Project Management Tools and Techniques , Strategic Planning & Goal Setting: Setting Business Goals
دبي	Systems Security Certified Practitioner SSCP
مانشستر - لندن	ITIL Foundation , CISSP Fast Track
مينارا (كوالالمبور)	[ITIL®]: Intermediate Lifecycle Service Operation , VM51IC - VMWare Vsphere: Install,Configure, Manage [V5.1]
لندن	TOGAF® Part 1&2 , Six Sigma Green Belt
سنغافورة	(SABSA Foundation (F1: Security Strategy and planing Module, F2 : Security Service Management and Design
جدة	التنظيم وتوزيع العمل

# 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.
- ← **الأقسام:** الموارد البشرية، 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 ١٤٣٤/١٤٣٥هـ (٢٠١٣ م)، وسيتهم في عام ٢٠١٤م، بإذن الله، الاستمرار في متابعة تنفيذ مشاريع المركز وتطويره والمشاركة في الفعاليات المحلية والدولية ذات العلاقة.