المملكة المغربية
البرلمان
مجلس المستشارين

تقـــرير

لجنة الخارجية والدفاع الوطني والمغاربة المقيمين في الخارج

حـــــــــول

مشروع قانون رقم 43.20 يتعلق بخدمات الثقة بشأن المعاملات الإلكترونية

رئيس اللجنة
محمد الرزمة

مقرر اللجنة
أحمد بولون

الأمانـــة العامـــــة
مديرية التشريع والمراقبة
قسم اللجان

مصلحة لجنة الخارجية والدفاع الوطني والمغاربة المقيمين في الخارج

الولاية التشريعية 2015 - 2021

السنة التشريعية 2020-2021

= دورة أكتوبر 2020 =

بطاقـــــة تقنيـــــة

- **رئيـــس اللجنـــــة** : المستشار محمد الرزمة

- **مقرر اللجنـــــــــة** : المستشار أحمد بولون

- **تاريخ الدراسة والتصويت على مشروع القانون** : الثلاثاء 15 ديسمبر 2020

- **عدد الاجتماعات** : 1

- **عدد ساعات العمل** : ساعتين و 15 دقيقة.

- **الطاقم الإداري الذي أعد التقرير** : تحت إشراف مقرر اللجنة

خالد طاهري (رئيس مصلحة اللجنة)

- **كريمة الزيانـــي**
- **محجوبة امطغري**

السيد الرئيس المحترم ،

السادة الوزراء المحترمون ،

السيدات والسادة المستشارون المحترمون ،

يشرفني أن أعرض على أنظار المجلس الموقر نص التقرير الذي أعدته لجنة الخارجية والدفاع الوطني والمغاربة المقيمين في الخارج حول مشروع قانون رقم 43.20 يتعلق بخدمات الثقة بشأن المعاملات الإلكترونية .

خصصت اللجنة يوم الثلاثاء 15 ديسمبر 2020 لدراسة مشروع القانون المذكور برئاسة السيد عمر مورو الخليفة الأول لرئيس اللجنة وحضور السيد عبد اللطيف لوديي الوزير المنتدب لدى رئيس الحكومة المكلف بإدارة الدفاع الوطني.

والذي قدم عرضا مستفيضا حول مشروع القانون ومراميه الأساسية حيث أوضح أنه يشكل لبنة أساسية ودعامة مهمة لباقي النصوص التشريعية المرتبطة بمجالي الأمن السيبراني والثقة الرقمية. ويتماشى مع التطور الرقمي الكبير الذي تعرفه بلادنا الأمر الذي يستدعي تهيئ مناخ للثقة يشمل جميع الخدمات الرقمية ويوفر للفاعلين الاقتصاديين والإدارات العمومية بيئة قانونية تساعد على إطلاق

خدمات جديدة، ويضمن في الوقت نفسه الحماية القانونية للمواطنين وتشجيعهم على الإقبال المتزايد على المعاملات الرقمية.

كما يهدف هذا المشروع قانون إلى وضع إطار قانوني جديد يستجيب لاحتياجات الفاعلين الاقتصاديين العموميين والخواص والإدارات العمومية والمواطنين، من خلال تنظيمه للتوقيعات الإلكترونية والخاتم الإلكتروني والختم الزمني الإلكتروني وخدمات الإرسال الإلكتروني المضمون والتيقن من مواقع الإنترنت.

ومن جهة أخرى يرمي إلى وضع إطار قانوني أقل تقييدا وأكثر ملائمة لمختلف المعاملات، وإلى توضيح الأثر القانوني للتوقيع الإلكتروني البسيط والمتقدم، بحيث لا يمكن رفض الأثر القانوني للتوقيعين الإلكترونيين، أو عدم قبولهما لمجرد تقديمهما في شكل إلكتروني أو لأنهما لا يفيان بمتطلبات التوقيع الإلكتروني المؤهل، هذا فضلا عن توسيع نطاق تطبيق القانون الحالي ليشمل المحررات المنجزة من لدن مؤسسات الائتمان والهيئات المعتبرة في حكمها.

وعند عرض مشروع قانون رقم 43.20 يتعلق بخدمات الثقة بشأن المعاملات الإلكترونية للتصويت مادة مادة والمشروع قانون برمته وافقت عليه اللجنة بإجماع أعضائها الحاضرين كما ورد عليها بدون تعديل.

إمضاء مقرر اللجنة

السيد أحمد بولون

عرض السيد الوزير

المملكة المغربية

إدارة الدفاع الوطني

عرض السيد الوزير المنتدب لدى رئيس الحكومة المكلف بإدارة الدفاع الوطني حول مشروع القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الالكترونية

لجنة الخارجية والدفاع الوطني والمغاربة المقيمين في الخارج
بمجلس المستشارين

الثلاثاء 15 دجنبر 2020

والصلاة والسلام على أشرف المرسلين وآله وصحبه

السيد رئيس اللجنة المحترم،

السيدات والسادة المستشارين المحترمين،

السيدات والسادة أطر مجلس المستشارين،

يسعدني أن أجدد اللقاء بكم في هذا الاجتماع الذي تخصصه لجنة الخارجية والدفاع الوطني والمغاربة المقيمين في الخارج بمجلس المستشارين لدراسة ومناقشة مشروع قانون رقم 43.20 يتعلق بخدمات الثقة بشأن المعاملات الإلكترونية والذي صادق عليه المجلس الوزاري المنعقد تحت رئاسة **صاحب الجلالة الملك محمد السادس نصره الله** بتاريخ 14 أكتوبر 2020، وحظي بالموافقة عليه بالإجماع من طرف مجلس النواب.

وقبل التطرق إلى سياق إعداد مشروع هذا القانون ومضامينه الأساسية، يطيب لي في مستهل هذه الكلمة أن أنتهز الفرصة لأعبر لكم ولكافة السيدات والسادة المستشارين المحترمين عن امتناني وتقديري لما تولونه من اهتمام بالغ ودعم متواصل لمقترحات ومبادرات إدارة الدفاع الوطني سواء أثناء مناقشة مشاريع القوانين التي تخص هذا القطاع أو من خلال دراسة ومناقشة الميزانية الفرعية لهذه الإدارة في إطار المصادقة على قانون المالية لكل سنة.

كما أغتنم هذه المناسبة لأتقدم إلى السيد رئيس اللجنة بخالص الشكر والامتنان على تفضله بإدارة أشغال هذه اللجنة وإلى السيدات والسادة الأعضاء الذين سيتفضلون بالمساهمة في مناقشة مشروع هذا القانون المعروض على أنظار لجنتكم الموقرة والشكر موصول كذلك للسيد المقرر الذي سيقوم بإعداد تقرير اللجنة حول هذا النص التشريعي.

السيد رئيس اللجنة المحترم،

السيدات والسادة المستشارين المحترمين،

في خضم التطور الذي يعرفه المجال الرقمي الذي يعد من أبرز الرهانات المستقبلية لبلادنا، أصبحت المعاملات الرقمية في مجالي التبادل والخدمات تحظى بأهمية كبرى. ومن أجل مسايرة التنمية الاقتصادية والاجتماعية الناتجة عن هذا التطور ومواكبة إصلاح الادارة وتبسيط المساطر، أصبح من الضروري تهيئ مناخ للثقة يشمل جميع الخدمات الرقمية، ويوفر للفاعلين الاقتصاديين والإدارات والهيئات العمومية بيئة قانونية تساعد على إطلاق خدمات جديدة،

مما سيضمن في نفس الوقت الحماية القانونية للمواطنين وتشجيعهم على الإقبال المتزايد على المعاملات الرقمية.

واعتبارا لكون هذه الثقة الرقمية تتجلى أساسا في الاستعمال الواسع للمصادقة الإلكترونية، أضحى لزاما مراجعة الإطار القانوني المنظم للتبادل الإلكتروني للمعطيات القانونية، من أجل تقديم بدائل أكثر ملاءمة للمستويات الأمنية التي يتطلبها استخدام الشهادات الإلكترونية، وذلك لتعزيز فعالية الخدمات العمومية والخاصة المقدمة عن بعد وإعطاء دفعة جديدة لتنمية النشاط الاقتصادي والتحول الرقمي في بلادنا.

ولهذا الغرض قامت إدارة الدفاع الوطني، بعد الموافقة **السامية لصاحب الجلالة الملك محمد السادس نصره الله**، بإعداد مشروع القانون المتعلق بخدمات الثقة بشأن المعاملات الالكترونية بعد التنسيق مع الوزارات والمؤسسات المعنية، بما في ذلك الهيئات التابعة للقطاع الخاص.

وبناء على ما سبق، اسمحوا لي السيد الرئيس المحترم، السيدات والسادة المستشارين المحترمين أن أتناول هذا العرض من خلال المحورين التاليين:

المحور الأول: يخص التجربة التي راكمتها بلادنا في ظل القانون الحالي رقم 53.05 والحاجة إلى تطوير شامل للمصادقة الإلكترونية

المحور الثاني: مستجدات مشروع القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الالكترونية

المحور الأول:
القانون رقم 53.05 بين التجربة التي راكمتها بلادنا والحاجة إلى تطوير شامل للمصادقة الإلكترونية

لقد شكل القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية أول إطار قانوني لاستعمال المصادقة الإلكترونية تم اعتماده ببلادنا سنة 2007، إلا أنه وبالرغم من إقرار هذا الإطار القانوني ونتيجة للتغيرات السريعة التي يعرفها مجال المعاملات الالكترونية، أضحت المصادقة الإلكترونية غير متطورة بالمستوى المطلوب ولم تعد ترقى إلى تطلعات واحتياجات المواطنين والإدارات والاقتصاد الوطني. حيث إن التشريع المؤطر للاستعمالات المرتبطة بالمصادقة الإلكترونية، فضل توفير أكبر قدر من الحماية الممكنة للمستعملين على حساب المرونة، الشيء الذي لم يسمح بتطوير أوسع للمصادقة الإلكترونية، ولم يكن يتوفر على آليات متعددة تغطي استعمالات مختلفة.

مع ذلك تميز القانون رقم 53.05 ببعض الإيجابيات نذكر منها ما يلي:

- اعتماد القاعدة التي تنص على أن الوثيقة المحررة بشكل إلكتروني لها نفس قوة إثبات الوثيقة المحررة على الورق، شريطة أن يكون بالإمكان التعرف، بصفة قانونية، على الشخص الذي صدرت عنه وأن تكون معدة ومحفوظة وفق شروط من شأنها ضمان تما ميتها؛
- الشهادات المؤمنة لا يمكن إصدارها إلا من طرف مقدم خدمات المصادقة الالكترونية المعتمد من قبل السلطة الوطنية المكلفة باعتماد ومراقبة المصادقة الإلكترونية.

ومنذ دخول هذا القانون حيز التطبيق، راكمت بلادنا تجربة متواضعة في هذا المجال، وهو ما دفع المصالح المختصة لتقييم هذه التجربة ومحاولة إغنائها، فبالإضافة إلى أن هذا القانون لم يكن مرنا بالشكل الذي يسمح بتطوير أوسع للمصادقة الإلكترونية، حيث اقتصرت المصادقة الإلكترونية على خدمة التوقيع الإلكتروني فقط، تميز هذا القانون ببعض النواقص التي أبانت الممارسة على ضرورة تجاوزها، ومن هذه النواقص ما يلي:

- التوقيع المؤمن لا يمكن اعتماده في جل الاستخدامات نظرا لما يتسم به من تعقيد من ناحية الكلفة والاجراءات بالإضافة إلى عدم الوضوح في تأطير بدائل لهذا التوقيع

بالشكل الكافي حتى تثبت صلاحيتها القانونية وتأخذ بعين الاعتبار مختلف مستويات المخاطر الممكنة (منخفض، متوسط أو عالي)؛

- التوقيع البسيط غير مؤطر بالشكل الكافي ويفتقر للوضوح مما جعل الفاعلين غير واثقين في قيمته القانونية ولم يتم استعماله في المستويات التي لا تتطلب التوقيع المؤمن؛
- هناك لبس في استعمال مرادف "مؤمن" مما يعطي الانطباع بأن باقي المستويات غير مؤمنة؛
- عدم تأطير باقي خدمات الثقة، على سبيل المثال **الخاتم الالكتروني، الختم الزمني الالكتروني** ...؛

المحور الثاني:

مستجدات مشروع القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الالكترونية

بناء على ما سبق، وأمام الحاجة الملحة لمراجعة القانون رقم 53.05 عبر تأطير خدمات الثقة الأخرى واللازمة في المعاملات الالكترونية، تم الحرص على إعداد مشروع القانون المعروض على أنظار لجنتكم الموقرة بتنسيق مع مختلف القطاعات والمصالح المعنية، حيث تمت صياغته في 84 مادة تم تقسيمها بشكل منهجي حسب محتوى ونوعية مواضيعها.

ومن أجل اطلاعكم على أهم مضامين مشروع هذا القانون سأتطرق في هذا المحور إلى نقطتين:

أولا: مرتكزات مشروع هذا القانون

عملت إدارة الدفاع الوطني على إعداد وصياغة مضامين مشروع هذا القانون من خلال الاعتماد على المرتكزات الأساسية التالية:

1. إطار قانوني جديد يستجيب لاحتياجات الفاعلين الاقتصاديين والإدارات

تم إعداد مشروع هذا القانون بناء على دراسة قامت بها إدارة الدفاع الوطني من أجل تحديد خريطة طريق تهدف إلى تطوير العرض المتعلق بالمصادقة الإلكترونية في بلادنا. وفي هذا الصدد، تم الحرص، أثناء جميع المراحل بدءا بجمع الاحتياجات ووصولا إلى مرحلة إعداد خريطة الطريق، على إجراء لقاءات مع عدة فاعلين اقتصاديين، وذلك من أجل تقييم مستوى تطور الاستخدامات الرقمية والتعرف بصورة محددة على احتياجاتهم الخاصة وتطلعاتهم في مجال الثقة الرقمية. وقد مكنت هذه اللقاءات من الاطلاع عن قرب على تصورهم للتطور الحالي للمصادقة الإلكترونية في المغرب والعوائق التي واجهتهم وكذا احتياجاتهم المستقبلية في هذا المجال.

2. إطار قانوني غني تم إعداده استئناسا بالتجارب الدولية المتقدمة في المجال

من أجل تعميق الدراسة تم الاعتماد على مقاربات مختلفة وعملية، وذلك عبر الاطلاع على التشريعات المقارنة لبعض الدول كالولايات المتحدة الأمريكية وكندا وفرنسا وماليزيا وكوريا الجنوبية.

كما تم الاستئناس باللائحة التنظيمية الصادرة عن الاتحاد الأوربي المتعلقة بخدمات الثقة بالنسبة للمعاملات الالكترونية والتي دخلت حيز التطبيق في فاتح يوليوز 2016، حيث شكلت إطارا تشريعيا مشتركا لدول الفضاء الأوروبي.

وفي ضوء التطور الذي عرفه هذا المجال على المستوى الدولي، أصبح من الواجب على بلادنا تحديث إطارها القانوني الحالي في مجال المعاملات الالكترونية، من أجل جعله متناسقا ومنسجما مع ما هو معتمد عند شركائنا الاقتصاديين .

3. إطار قانوني جديد، أقل تقييدا، أكثر شمولية، وأكثر ملاءمة لمختلف الاستخدامات

إن الاعتماد في إطار التشريع المقترح على نظام أقل تقييدا من النظام الحالي، سيسمح برقمنة غالبية الاستخدامات التي تعرف مخاطر ذات مستوى منخفض أو متوسط (مستوى غير مؤهل)، مع الحفاظ على نظام أكثر صرامة لتغطية الاستخدامات ذات المخاطر العالية (مستوى مؤهل).

علاوة على ذلك، أبانت الظروف التي تعيشها بلادنا بسبب جائحة كورونا وإصلاح الإدارة وتبسيط المساطر عن الحاجة إلى تطوير سريع للخدمات الالكترونية حتى يتمكن المواطنون من استخدامها للتواصل مع السلطات العمومية وتمكين الإدارة والفاعلين الاقتصاديين العموميين والخواص من تطوير الخدمات عن بعد ورقمنة المساطر، وبالتالي المساهمة في تسريع التحول الرقمي للمملكة.

وفي إطار الاستجابة للإكراهات القانونية الحالية وتغطية جل الاحتياجات، سيمكن مشروع هذا القانون من ضمان الثقة في المعاملات الالكترونية عبر اقتراح ثلاث مستويات للتوقيع الالكتروني:

المستوى البسيط:

- لا يتطلب شروطا تقنية أو عملية محددة من أجل استخدام عادي؛
- لا يتطلب قرينة الموثوقية : عبء الاثبات يقع على عاتق المدعى عليه.

ويمكن أن يغطي هذا المستوى: التصريحات ذات الرهانات المتوسطة، والعقود ذات الرهانات المنخفضة كطلبات القروض البنكية والتصريحات التي تخص الضرائب والضمان الاجتماعي والاستشارات الإدارية.

المستوى المتقدم:

- يتميز باعتراف قانوني يفوق ذلك المخصص للمستوى البسيط : شروط تقنية وتنظيمية للمستوى المتوسط (يرتكز على شهادة إلكترونية غير مؤهلة) أكثر مرونة من التوقيع المؤهل؛
- مفيد لتطوير استخدامات ذات رهان متوسط؛
- لا يوجب قرينة الموثوقية : عبء الاثبات يقع على عاتق المدعى عليه.

بخصوص هذا المستوى، يمكن أن يهم: التصريحات ذات الرهانات المتوسطة، شهادات ذات الرهانات المتوسطة (كالضمان الاجتماعي والضرائب وشهادة التسجيل....)، العقود ذات الرهانات العالية (كالتأمين والقروض البنكية....)، الشهادات المدنية أو العقود القانونية ذات رهانات متوسطة، الاجابة على الصفقات العمومية.

المستوى المؤهل:

- يشترط وجوبا استعمال وسائل التشفير (***moyens de cryptologie***) ؛
- يستفيد من قرينة الموثوقية؛
- مفيد لتطوير استخدامات ذات رهان جد قوي.

يمكن أن تندرج في هذا المستوى المعاملات التالية: شهادات ذات رهانات عالية، ارسال الملفات القانونية، العقود، المعاملات البنكية ذات رهانات عالية (المبالغ الكبيرة، ....)، توقيع العقود المتعلقة بالصفقات العمومية.

إضافة إلى ما سبق، فإن مشروع هذا القانون قد تضمن مستجدات، ستجعله أكثر شمولية للمعاملات الالكترونية، لا سيما من خلال تنظيمه لخدمات ثقة جديدة أصبحت ضرورية لتأمين المعاملات الإلكترونية، وتشمل هذه الخدمات:

- الخاتم الإلكتروني (***Cachet électronique***) الذي يمكن من ضمان أصل المعطيات الإلكترونية وتماميتها؛
- الختم الزمني الإلكتروني (***Horodatage électronique***) الذي يتجلى في معطيات على شكل إلكتروني ترتبط بلحظة زمنية معينة وتشكل حجة على كون هذه المعطيات كانت موجودة في تلك اللحظة بالذات؛

- خدمات الإرسال الإلكتروني المضمون *(Services d'envoi recommandé électronique)* والتي تسمح بإرسال المعطيات بطريقة إلكترونية وتقدم الحجج المتعلقة بمعالجة المعطيات المرسلة بما فيها حجة إرسالها وتلقيها وتحمي المعطيات المرسلة من أخطار الضياع أو السرقة أو التلف أو كل تغيير غير مأذون به؛
- التيقن من مواقع الانترنت *(Authentification des sites internet)* من خلال شهادات مؤهلة للتيقن من هذه المواقع وتسمح هذه الشهادات بالتحقق من صدقية هذه المواقع وربطها بالأشخاص الذاتيين أو الاعتباريين المسلمة إليهم هذه الشهادات من طرف مقدمي خدمات ثقة معتمدين.

ثانيا: أهم مضامين مشروع هذا القانون

1. تحديد خدمات الثقة

يحدد مشروع القانون هذه الخدمات فيما يلي:

✓ **إنشاء التوقيعات الإلكترونية** *(création de signatures électroniques)*، **والأختام الإلكترونية** *(cachets électroniques)*، **والختم الزمني الإلكتروني** *(horodatage électronique)*، **وخدمات الإرسال الإلكتروني المضمون** *(services d'envoi recommandé électronique)*: تتميز هذه الخدمات بكونها ترتكز على عمليات تقنية يصعب تزويرها.

✓ **إنشاء الشهادات المتعلقة بالتوقيعات الإلكترونية** *(création des certificats relatifs aux signatures électroniques)*، **وبالأختام الإلكترونية** *(cachets électroniques)*، **وبالختم الزمني الإلكتروني** *(horodatage électronique)* **وبالتيقن من مواقع الأنترنت** *(authentification des sites internet)*: هذه الشهادات عبارة عن ملف إلكتروني يحتوي خصوصا على المعلومات الشخصية لصاحب الشهادة، والمعلومات المتعلقة بمقدم خدمات الثقة ومعلومات أخرى، بالإضافة إلى مفتاح الشفرة العمومي الذي يرتبط منطقيًا بمفتاح الشفرة الخاص.

يمكن أن تكون هذه الشهادات إما على شكل برمجية أوعلى شكل آلية (بطاقة ذكية، أداة مشفرة،...)

✓ **إثبات صحة التوقيعات الإلكترونية والأختام الإلكترونية** *(validation de signatures électroniques)*

(*électroniques ou de cachets électroniques*) : تتجلى أهمية إثبات صحة التوقيع الإلكتروني أو الختم الإلكتروني في التحقق من صحة التوقيع أو الخاتم بمجرد وضعها على الوثيقة، لأن مدة صلاحية الشهادة الالكترونية لا تتجاوز عموما ثلاث سنوات، وسيكون من الصعب التحقق من صحتها بعد انتهاء مدة الصلاحية.

✓ **حفظ التوقيعات الإلكترونية والأختام الإلكترونية والشهادات المتعلقة بهاتين الخدمتين** (*conservation de signatures électroniques, de cachets électroniques ou de certificats relatifs à ces services*) : تهدف هذه العملية إلى الحفاظ على موثوقية التوقيع الإلكتروني أو الخاتم الإلكتروني إلى ما بعد فترة الصلاحية التكنولوجية للتقنيات المستعملة. مما يمكن من إبقاء القوة الثبوتية للوثيقة الإلكترونية. كما تساعد هذه الخدمة على الحماية من التقادم التكنولوجي أو من خرق الخوارزميات المستخدمة في التوقيعات أو الأختام الإلكترونية.

2. تحديد النظام المطبق على خدمات الثقة بشأن المعاملات الالكترونية وعلى وسائل وخدمات التشفير وتحليل الشفرات

وفي هذا السياق، يرمي مشروع هذا القانون إلى سن القواعد المطبقة على خدمات الثقة وعلى مقدمي هذه الخدمات لإضفاء ثقة أكبر على هذا المجال. ولهذه الغاية تم التنصيص في هذا المشروع على خضوع جميع مقدمي خدمات الثقة لمقتضيات محددة، لا سيما في مجال الأمن والمسؤولية المرتبطة بأنشطتهم وخدماتهم.

ونظرا للتنوع والاختلاف الذي تعرفه خدمات الثقة، يميز هذا المشروع بين مقدمي خدمات الثقة المعتمدين من جهة، ومقدمي خدمات الثقة غير المعتمدين من جهة أخرى. ولذلك، تم اقتراح نظامين لتأطير مقدمي الخدمات:

- نظام يستفيد من ثقة أكبر مع خضوعه لمتطلبات صارمة مرتبطة بضرورة الحصول على الاعتماد من السلطة الوطنية لخدمات الثقة، ولا يمكن تقديم خدمة ثقة مؤهلة، وإصدار شهادات إلكترونية مؤهلة وتسليمها وتدبير العمليات المتعلقة بها، إلا من لدن مقدمي خدمات ثقة المعتمدين وفق الشروط المحددة في القانون؛

- نظام مخفف يرتكز على التصريح ولا يتطلب أي اعتماد، وفي إطاره يمكن لكل شخص يرغب في تقديم خدمات ثقة لا تدخل ضمن الخدمات المؤهلة، التصريح مسبقا بذلك لدى السلطة الوطنية.

أما فيما يتعلق بمراقبة التشفير وتحليل الشفرات، ينص هذا المشروع على اعتماد إطار تشريعي يجعل هذه المراقبة مقتصرة على كل ما من شأنه المساس بمصالح الدفاع وأمن الدولة.

3. تحديد اختصاصات السلطة الوطنية لخدمات الثقة بشأن المعاملات الالكترونية

ومن أجل التنفيذ الفعال والملائم لمختلف الأحكام التي جاء بها مشروع هذا القانون، يعهد إلى **السلطة الوطنية لخدمات الثقة بشأن المعاملات الإلكترونية**، على الخصوص، ممارسة المهام التالية:

- تحديد المعايير والدلائل المرجعية المطبقة على خدمات الثقة المذكورة، واتخاذ التدابير اللازمة لتنفيذها؛
- اعتماد مقدمي خدمات الثقة المؤهلة المستوفين للشروط المحددة في القانون، من أجل تقديم خدمات ثقة مؤهلة وإصدار شهادات إلكترونية مؤهلة وتسليمها وتدبير العمليات المتعلقة بها، ومراقبة أنشطتهم؛
- المراقبة البعدية لمقدمي خدمات الثقة غير المعتمدين، حيث يمكن للسلطة الوطنية، إما تلقائيا وإما بطلب من أي شخص يهمه الأمر، أن تراقب أو أن تعمل على مراقبة مطابقة أنشطة مقدم خدمات الثقة لأحكام هذا القانون والنصوص المتخذة لتطبيقه.
- اقتراح مشاريع النصوص التشريعية والتنظيمية المتعلقة بخدمات الثقة بشأن المعاملات الإلكترونية.
- السماح باستيراد وسائل التشفير وتحليل الشفرات أو تصديرها أو توريدها وكذا تقديم خدمات التشفير وتحليل الشفرات، من خلال تلقي التصريح المسبق عندما ينحصر الغرض من هذه الوسيلة أو هذه الخدمة في التيقن من إرسالية أو ضمان تمامية المعطيات المرسلة بطريقة إلكترونية، ومنح التراخيص عندما يتعلق الأمر بغرض غير هذه الأغراض.

وملاءمة مع الواقع العملي، كان لا بد من تحيين بعض **أحكام قانون الالتزامات والعقود**، وذلك بتغيير الفصل 2.1 (الفقرة 3) بإضافة المحررات المنجزة من لدن مؤسسات الائتمان والهيئات المعتبرة في حكمها في نطاق تطبيق أحكام هذا القانون لكون هذه المعاملات جاري بها العمل يوميا في القطاع الاقتصادي ويجب أن تستفيد أيضًا من الحماية القانونية التي يوفرها هذا القانون.

ومن أجل ضمان الأمن القانوني للهيئات التي تستخدم حاليا شهادات مؤمنة تم تسليمها، قبل اعتماد مشروع هذا القانون وفقا لمتطلبات التشريع الجاري به العمل في مجال التبادل الإلكتروني للمعطيات القانونية، تم الحرص على التنصيص في مشروع هذا القانون على أحكام انتقالية تضمن سريان مفعول هذه الشهادات.

السيد رئيس اللجنة المحترم،
السيدات والسادة المستشارين المحترمين،

من خلال ما سبق وما تمت الإشارة إليه في هذا العرض، فإن مشروع هذا القانون سيشكل لبنة أساسية ودعامة مهمة لباقي النصوص القانونية المرتبطة بمجالي الأمن السيبراني والثقة الرقمية.

وهكذا سيساهم مشروع هذا القانون في تكريس الثقة في المعاملات الالكترونية ليس فقط على المستوى الوطني، وإنما في علاقتنا مع شركائنا، في استجابة للتطلعات والاحتياجات المتعددة المعبر عنها من لدن الفاعلين الاقتصاديين والإدارات، وسيسمح بتأطير خدمات الثقة الأخرى واللازمة في المعاملات الالكترونية، وذلك من أجل تعزيز فعالية الخدمات العمومية والخاصة وكذا تطوير الخدمات المقدمة عن بعد حتى يتسنى إعطاء دفعة جديدة لتنمية النشاط الاقتصادي والتحول الرقمي في بلادنا.

وفي ختام هذا العرض، اسمحوا لي أن أتقدم إليكم بالشكر الجزيل على حسن اهتمامكم، وعلى دعمكم ومساندتكم وتفاعلكم الإيجابي مع مشاريع القوانين التي تعدها إدارة الدفاع الوطني.

والسلام عليكم ورحمة الله تعالى وبركاته

مشروع القانون

كما أحيل على اللجنة ووافقت عليه

المملكة المغربية
البرلمان
مجلس النواب

مشروع قانون رقم 43.20
يتعلق بخدمات الثقة بشأن المعاملات الإلكترونية

(كما وافق عليه مجلس النواب في 08 دجنبر 2020)

نسخة مطابقة لأصل النص
كما وافق عليه مجلس النواب

الحبيب المالكي
رئيس مجلس النواب

مشروع قانون رقم 43.20
يتعلق بخدمات الثقة
بشأن المعاملات الإلكترونية

قسم تمهيدي

أحكام عامة

المادة الأولى

يهدف هذا القانون إلى تحديد النظام المطبق على خدمات الثقة بشأن المعاملات الإلكترونية، وعلى وسائل وخدمات التشفير وتحليل الشفرات وكذا على العمليات المنجزة من قبل مقدمي خدمات الثقة والقواعد الواجب التقيد بها من لدن هؤلاء ومن لدن أصحاب الشهادات الإلكترونية.

ويحدد كذلك اختصاصات السلطة الوطنية لخدمات الثقة بشأن المعاملات الإلكترونية المعينة بنص تنظيمي والمشار إليها في هذا القانون «بالسلطة الوطنية».

المادة 2

يراد في مدلول هذا القانون بما يلي :

- **المعاملات الإلكترونية** : كل تبادل أو مراسلة أو عقد أو وثيقة، أو أي معاملة أخرى تبرم أو تنفذ بطريقة إلكترونية بشكل كلي أو جزئي ؛
- **الطريقة الإلكترونية** : كل وسيلة ترتبط بتقنية ذات قدرات كهربائية أو رقمية أو مغناطيسية أو لاسلكية أو بصرية أو كهرومغناطيسية أو أي قدرات أخرى مماثلة ؛
- **التعريف الإلكتروني** : سلسلة من العمليات تتجلى في استخدام معطيات تعريف شخصية في شكل إلكتروني تدل، بما لا يدع مجالا للشك، على شخص ذاتي أو اعتباري دون غيره، أو على شخص ذاتي يمثل شخصا اعتباريا ؛
- **التيقن** : سلسلة من العمليات الإلكترونية تسمح بتأكيد التعريف الإلكتروني لشخص ذاتي أو اعتباري، أو أصل المعطيات في شكل إلكتروني وتماميتها ؛
- **الطرف المستعمل** : كل شخص ذاتي أو اعتباري يثق في خدمة من خدمات الثقة ؛
- **صاحب التوقيع** : كل شخص ذاتي ينشئ توقيعا إلكترونيا ؛
- **التوقيع الإلكتروني البسيط** : توقيع يتجلى في استعمال طريقة ذات موثوقية للتعريف الإلكتروني تضمن ارتباط التوقيع بالوثيقة المتعلقة به، ويعبر عن رضى صاحب التوقيع ؛
- **معطيات إنشاء التوقيع الإلكتروني** : معطيات فريدة تستعمل من لدن صاحب التوقيع من أجل إنشاء توقيع إلكتروني ؛
- **شهادة التوقيع الإلكتروني** : شهادة إلكترونية تربط معطيات إثبات صحة التوقيع الإلكتروني بشخص ذاتي، والتي تؤكد على الأقل اسم الشخص المذكور، أو اسمه المستعار عند الاقتضاء ؛
- **آلية إنشاء التوقيع الإلكتروني**: كل معدات أو برمجيات، أو هما معا، تتضمن العناصر المميزة الخاصة بصاحب التوقيع والمعدة لتوظيف معطيات إنشاء التوقيع الإلكتروني والمستخدمة في إنشائه ؛
- **الخاتم الإلكتروني البسيط** : معطيات في شكل إلكتروني تم إنشاؤها من قبل شخص اعتباري تكون مرفقة بمعطيات أخرى في شكل إلكتروني أو مرتبطة بها منطقيا، من أجل ضمان أصل هذه الأخيرة وتماميتها ؛
- **معطيات إنشاء الخاتم الإلكتروني** : معطيات فريدة تستعمل من طرف منشئ الخاتم الإلكتروني من أجل إنشاء خاتم إلكتروني؛
- **شهادة الخاتم الإلكتروني** : شهادة إلكترونية تربط معطيات إثبات صحة خاتم إلكتروني بشخص اعتباري وتؤكد تسميته ؛
- **آلية إنشاء الخاتم الإلكتروني** : كل المعدات أو البرمجيات، أو هما معا، التي تتضمن العناصر المميزة الخاصة بمنشئ الخاتم والمعدة لتوظيف معطيات إنشاء الخاتم الإلكتروني والمستخدمة في إنشائه ؛
- **مقدم خدمات ثقة** : كل شخص اعتباري يقدم خدمة أو أكثر من خدمات الثقة ويمكن أن يكون معتمدا أو غير معتمد ؛
- **إثبات الصحة** : سلسلة من عمليات التحقق أو التأكد من صحة توقيع إلكتروني أو خاتم إلكتروني.

المادة 3

تتمثل خدمات الثقة في ما يلي :

- إنشاء التوقيعات الإلكترونية، أو الأختام الإلكترونية، أو الختم الزمني الإلكتروني، أو خدمات الإرسال الإلكتروني المضمون ؛

- إنشاء الشهادات المتعلقة بالتوقيعات الإلكترونية، أو بالأختام الإلكترونية، أو بالختم الزمني الإلكتروني أو بالتيقن من مواقع الأنترنت ؛

- إثبات صحة التوقيعات الإلكترونية أو الأختام الإلكترونية ؛

- حفظ التوقيعات الإلكترونية أو الأختام الإلكترونية أو الشهادات المتعلقة بهاتين الخدمتين.

القسم الأول

النظام المطبق على خدمات الثقة بشأن المعاملات الإلكترونية وعلى وسائل وخدمات التشفير وتحليل الشفرات

الباب الأول

خدمات الثقة بشأن المعاملات الإلكترونية ومقدمو خدمات الثقة والتزامات صاحب الشهادة الإلكترونية

الفرع الأول

خدمات الثقة

القسم الفرعي الأول

التوقيع الإلكتروني

المادة 4

يكون التوقيع الإلكتروني إما بسيطا أو متقدما أو مؤهلا.

المادة 5

التوقيع الإلكتروني المتقدم هو توقيع إلكتروني بسيط، كما تم تعريفه في المادة 2 أعلاه، يستوفي الشروط التالية :

- أن يكون خاصا بصاحب التوقيع ؛

- أن يسمح بتحديد هوية الموقع ؛

- أن يتم إنشاؤه بواسطة معطيات إنشاء التوقيع الإلكتروني التي يمكن أن يستعملها صاحب التوقيع تحت مراقبته بصفة حصرية، وبدرجة عالية من الثقة تحدد من قبل السلطة الوطنية ؛

- أن يرتكز على شهادة إلكترونية أو بكل وسيلة تعتبر معادلة لها تحدد بنص تنظيمي ؛

- وأن يكون مرتبطا بالمعطيات المتعلقة بهذا التوقيع بكيفية تمكن من كشف كل تغيير لاحق يطرأ عليها.

المادة 6

التوقيع الإلكتروني المؤهل هو توقيع إلكتروني متقدم يجب إنتاجه بواسطة آلية لإنشاء التوقيع الإلكتروني المؤهلة المنصوص عليها في المادة 8 بعده، والذي يستند إلى شهادة مؤهلة للتوقيع الإلكتروني كما هو منصوص عليها في المادة 9 أدناه.

المادة 7

لا يمكن رفض الأثر القانوني للتوقيع الإلكتروني البسيط أو المتقدم كحجة أمام القضاء أو عدم قبوله لمجرد تقديم هذا التوقيع في شكل إلكتروني، أو لأنه لا يفي بمتطلبات التوقيع الإلكتروني المؤهل المنصوص عليه في المادة 6 أعلاه.

المادة 8

آلية إنشاء التوقيع الإلكتروني المؤهلة هي آلية إنشاء التوقيع الإلكتروني المثبتة بشهادة للمطابقة مسلمة من لدن السلطة الوطنية. ويجب أن تستجيب هذه الآلية للمتطلبات التالية:

- أن تضمن بوسائل تقنية وإجراءات ملائمة، عدم إمكانية التوصل إلى معطيات إنشاء التوقيع الإلكتروني عن طريق الاستنباط، وإمكانية حماية التوقيع الإلكتروني من أي تزوير، بكيفية موثوق بها وبواسطة الوسائل التقنية المتاحة ؛

- أن تضمن بوسائل تقنية وإجراءات ملائمة، أن معطيات إنشاء التوقيع الإلكتروني لا يمكن إعدادها أكثر من مرة واحدة وتكون سريتها مضمونة ويمكن حمايتها من قبل صاحب التوقيع بكيفية مقبولة من أي استعمال من لدن الغير ؛

- ألا تؤدي إلى أي تلف لمحتوى الوثيقة الإلكترونية المراد توقيعها أو تغييره، وألا تشكل عائقا يحول دون أن يكون لصاحب التوقيع إلمام تام بمحتوى الوثيقة قبل توقيعها.

علاوة على ذلك، لا يمكن أن يعهد بتوليد معطيات إنشاء التوقيع الإلكتروني المؤهل أو تدبيرها لحساب صاحب التوقيع إلا لمقدم خدمات ثقة معتمد وفقا لأحكام المادة 33 من هذا القانون.

تقوم السلطة الوطنية بنشر لائحة آليات إنشاء التوقيع الإلكتروني المؤهلة على موقع الأنترنت الخاص بها.

المادة 9

تسلم شهادة التوقيع الإلكتروني المؤهلة من قبل مقدم خدمات ثقة معتمد، وتتضمن معطيات ومعلومات تحدد بنص تنظيمي.

المادة 10

تؤكد عملية إثبات صحة توقيع إلكتروني مؤهل صحة هذا التوقيع، شريطة :

- أن تكون الشهادة التي استند إليها التوقيع، أثناء التوقيع، شهادة مؤهلة للتوقيع الإلكتروني وفقا لأحكام المادة 9 أعلاه ؛
- أن تكون الشهادة المؤهلة مسلمة من لدن مقدم خدمات ثقة معتمد وصالحة أثناء التوقيع ؛
- أن تكون معطيات إثبات صحة التوقيع مطابقة للمعطيات التي تم إرسالها إلى الطرف المستعمل ؛
- أن تقدم بشكل صحيح للطرف المستعمل المجموعة الفريدة للمعطيات التي تدل على صاحب التوقيع في الشهادة ؛
- أن يتم، في حالة استعمال اسم مستعار أثناء التوقيع، إخبار الطرف المستعمل بذلك بشكل واضح ؛
- أن يتم إنشاء التوقيع الإلكتروني بواسطة آلية لإنشاء التوقيع الإلكتروني مؤهلة وأن يتم استيفاء الشروط المنصوص عليها في المادة 5 من هذا القانون عند التوقيع ؛
- ألا يشوب تمامية المعطيات الموقعة أي اختلال.

علاوة على ذلك، يجب أن يقدم النظام المستعمل لإثبات صحة التوقيع الإلكتروني المؤهل إلى الطرف المستعمل النتيجة الصحيحة لسلسلة عمليات إثبات الصحة، وأن يسمح له برصد أي مشكل وجيه يتعلق بسلامة سلسلة العمليات المذكورة.

المادة 11

لا يمكن تقديم خدمة مؤهلة لإثبات صحة التوقيعات الإلكترونية المؤهلة إلا من لدن مقدم خدمات ثقة معتمد :

- يقدم خدمة إثبات الصحة وفقا لأحكام المادة 10 أعلاه ؛
- ويسمح للطرف المستعمل بتلقي نتيجة مجموع عمليات إثبات الصحة بطريقة آلية وذات موثوقية وفعالة، وتحمل التوقيع الإلكتروني المتقدم لمقدم الخدمات المذكور أو خاتمه الإلكتروني المتقدم.

المادة 12

لا يمكن تقديم خدمة حفظ مؤهلة للتوقيعات الإلكترونية المؤهلة، إلا من قبل مقدم خدمات ثقة معتمد، يستعمل مساطر وتكنولوجيات تسمح بتمديد موثوقية التوقيع الإلكتروني المؤهل إلى ما بعد الصلاحية التكنولوجية.

القسم الفرعي الثاني

الخاتم الإلكتروني

المادة 13

يكون الخاتم الإلكتروني إما بسيطا أو متقدما أو مؤهلا.

المادة 14

الخاتم الإلكتروني المتقدم هو خاتم إلكتروني بسيط، كما تم تعريفه في المادة 2 من هذا القانون، يستوفي الشروط التالية :

- أن يكون خاصا بمنشئ الخاتم بما لا يدع مجالا للشك ؛
- أن يسمح بتحديد هوية منشئ الخاتم ؛
- أن يتم إنشاؤه بواسطة معطيات إنشاء الخاتم الإلكتروني التي يمكن أن يستعملها منشئ الخاتم تحت مراقبته وبدرجة عالية من الثقة تحدد من قبل السلطة الوطنية ؛
- أن يرتكز على شهادة إلكترونية أو بكل وسيلة تعتبر معادلة لها تحدد بنص تنظيمي ؛
- وأن يكون مرتبطا بالمعطيات المتعلقة بهذا الخاتم بكيفية تمكن من كشف كل تغيير لاحق يطرأ عليها.

المادة 15

الخاتم الإلكتروني المؤهل هو خاتم إلكتروني متقدم يجب إنتاجه بواسطة آلية إنشاء الخاتم الإلكتروني المؤهلة والمنصوص عليها في المادة 17 بعده، والذي يستند إلى شهادة خاتم إلكتروني مؤهلة كما هو منصوص عليها في المادة 18 أدناه.

يتمتع الخاتم الإلكتروني المؤهل بقرينة تمامية المعطيات التي يرتبط بها وبدقة مصدر هذه المعطيات.

المادة 16

لا يمكن رفض الأثر القانوني للخاتم الإلكتروني البسيط أو المتقدم كحجة أمام القضاء أو عدم قبوله لمجرد تقديم هذا الخاتم في شكل إلكتروني أو لأنه لا يفي بمتطلبات الخاتم الإلكتروني المؤهل المنصوص عليه في المادة 15 أعلاه.

المادة 17

آلية إنشاء الختم الإلكتروني المؤهلة هي آلية إنشاء ختم إلكتروني مثبتة بشهادة للمطابقة مسلمة من لدن السلطة الوطنية. ويجب أن تستجيب هذه الآلية للمتطلبات التالية :

- أن تضمن بوسائل تقنية وإجراءات ملائمة، عدم إمكانية التوصل إلى معطيات إنشاء الختم الإلكتروني عن طريق الاستنباط، وإمكانية حماية الختم الإلكتروني من أي تزوير، بكيفية موثوق بها وبواسطة الوسائل التقنية المتاحة ؛

- وأن تضمن بوسائل تقنية وإجراءات ملائمة، أن معطيات إنشاء الختم الإلكتروني لا يمكن إعدادها أكثر من مرة واحدة وتكون سريتها مضمونة ويمكن حمايتها من قبل منشئ الختم بكيفية مقبولة من أي استعمال من لدن الغير ؛

- وألا تؤدي إلى أي تلف لمحتوى الوثيقة المراد ختمها أو تغييره وألا تشكل عائقا يحول دون أن يكون لمنشئ الختم إلمام تام بمحتوى الوثيقة قبل ختمها.

علاوة على ذلك، لا يمكن أن يعهد بتوليد معطيات إنشاء الختم الإلكتروني المؤهل أو تدبيرها لحساب منشئ الختم إلا لمقدم خدمات ثقة معتمد وفقا لأحكام المادة 33 من هذا القانون.

تقوم السلطة الوطنية بنشر لائحة آليات إنشاء الختم الإلكتروني المؤهلة على موقع الأنترنت الخاص بها.

المادة 18

تسلم شهادة الختم الإلكتروني المؤهلة من لدن مقدم خدمات ثقة معتمد، وتتضمن معطيات ومعلومات تحدد بنص تنظيمي.

المادة 19

تؤكد عملية إثبات صحة ختم إلكتروني مؤهل صحة هذا الختم، شريطة :

- أن تكون الشهادة التي استند إليها الختم، أثناء إنشاء الختم، شهادة مؤهلة للختم الإلكتروني وفقا لأحكام المادة 18 أعلاه ؛

- أن تكون الشهادة المؤهلة مسلمة من لدن مقدم خدمات ثقة معتمد وصالحة أثناء إنشاء الختم ؛

- أن تكون معطيات إثبات صحة الختم الإلكتروني مطابقة للمعطيات التي تم إرسالها إلى الطرف المستعمل ؛

- أن تقدم بشكل صحيح للطرف المستعمل المجموعة الفريدة للمعطيات التي تدل على منشئ الختم في الشهادة ؛

- أن يتم إنشاء الختم الإلكتروني بواسطة آلية إنشاء الختم الإلكتروني المؤهلة، وأن يتم استيفاء الشروط المنصوص عليها في المادة 14 من هذا القانون عند إنشاء الختم ؛

- ألا يشوب تمامية المعطيات المختومة أي اختلال.

علاوة على ذلك، يجب أن يقدم النظام المستعمل لإثبات صحة الختم الإلكتروني المؤهل إلى الطرف المستعمل النتيجة الصحيحة لسلسلة عمليات إثبات الصحة، وأن يسمح له برصد أي مشكل وجيه يتعلق بسلامة سلسلة العمليات المذكورة.

المادة 20

لا يمكن تقديم خدمة مؤهلة لإثبات صحة الخواتم الإلكترونية المؤهلة إلا من لدن مقدم خدمات ثقة معتمد :

- يقدم خدمة إثبات الصحة وفقا لأحكام المادة 19 أعلاه ؛

- يسمح للطرف المستعمل بتلقي نتيجة مجموع عمليات إثبات الصحة، بطريقة آلية وذات موثوقية وفعالة، وتحمل التوقيع الإلكتروني المتقدم لمقدم الخدمات المذكور أو خاتمه الإلكتروني المتقدم.

المادة 21

لا يمكن تقديم خدمة حفظ مؤهلة للأختام الإلكترونية المؤهلة، إلا من قبل مقدم خدمات ثقة معتمد، يستعمل مساطر وتكنولوجيات تسمح بتمديد موثوقية الأختام الإلكترونية المؤهلة إلى ما بعد الصلاحية التكنولوجية.

القسم الفرعي الثالث

الختم الزمني الإلكتروني

المادة 22

يكون الختم الزمني الإلكتروني إما بسيطا أو مؤهلا.

المادة 23

يتجلى الختم الزمني الإلكتروني البسيط في معطيات على شكل إلكتروني تربط معطيات أخرى على شكل إلكتروني بلحظة زمنية معينة وتشكل حجة على كون هذه المعطيات كانت موجودة في تلك اللحظة بالذات.

المادة 24

الختم الزمني الإلكتروني المؤهل هو ختم زمني إلكتروني بسيط، يستوفي الشروط التالية :

- أن يربط التاريخ والساعة بالمعطيات بكيفية تسمح باستبعاد إمكانية حدوث أي تغيير في المعطيات غير قابل للكشف عنه ؛
- أن يستند إلى ساعة مضبوطة مرتبطة بالتوقيت العالمي المنسق ؛
- وأن يكون موقعا بواسطة توقيع إلكتروني متقدم أو مختوما بواسطة خاتم إلكتروني متقدم من لدن مقدم خدمات ثقة معتمد.

يتمتع الختم الزمني الإلكتروني المؤهل بقرينة دقة التاريخ والساعة الذي يشير إليهما، وكذا بتمامية المعطيات المرتبطة بهذا التاريخ وبهذه الساعة.

المادة 25

لا يمكن رفض الأثر القانوني للختم الزمني الإلكتروني البسيط كحجة أمام القضاء أو عدم قبوله لمجرد تقديم هذا الختم الزمني في شكل إلكتروني أو لأنه لا يفي بمتطلبات الختم الزمني الإلكتروني المؤهل المنصوص عليه في المادة 24 أعلاه.

القسم الفرعي الرابع

خدمة الإرسال الإلكتروني المضمون

المادة 26

تكون خدمة الإرسال الإلكتروني المضمون إما بسيطة أو مؤهلة.

المادة 27

تسمح خدمة الإرسال الإلكتروني المضمون البسيطة بإرسال المعطيات بطريقة إلكترونية، وتقدم الحجج المتعلقة بمعالجة المعطيات المرسلة بما فيها حجة إرسالها وتلقيها، وتحمي المعطيات المرسلة من أخطار الضياع أو السرقة أو التلف أو كل تغيير غير مأذون به.

المادة 28

خدمة الإرسال الإلكتروني المضمون المؤهلة هي خدمة إرسال إلكتروني مضمون بسيطة، تستوفي الشروط التالية :

- أن تقدم من لدن واحد أو أكثر من مقدمي خدمات ثقة معتمدين ؛
- أن تضمن تحديد هوية المرسل بدرجة عالية من الثقة تحدد من قبل السلطة الوطنية ؛
- أن تضمن تحديد هوية المرسل إليه قبل تسليم المعطيات ؛
- أن تضمن سلامة إرسال المعطيات والتوصل بها بواسطة توقيع إلكتروني متقدم أو خاتم إلكتروني متقدم، بكيفية تسمح باستبعاد إمكانية حدوث أي تغيير في المعطيات غير قابل للكشف عنه ؛
- أن تسمح بإشعار المرسل والمرسل إليه، بشكل واضح، بكل تغيير للمعطيات يكون ضروريا لإرسالها أو التوصل بها ؛
- أن تشير بواسطة ختم زمني إلكتروني مؤهل إلى تاريخ الإرسال والتوصل وساعتهما، وإلى كل تغيير في المعطيات.

تتمتع المعطيات المرسلة والمتوصل بها بواسطة خدمة الإرسال الإلكتروني المضمون المؤهلة بقرينة تماميتها، وإرسالها من لدن مرسل محدد الهوية والتوصل بها من طرف مرسل إليه محدد الهوية، ودقة تاريخ وساعة الإرسال والتوصل المشار إليهما في الخدمة المذكورة.

المادة 29

لا يمكن رفض الأثر القانوني للمعطيات المرسلة والمتوصل بها بواسطة خدمة الإرسال الإلكتروني المضمون البسيطة كحجة أمام القضاء أو عدم قبوله لمجرد تقديم هذه الخدمة في شكل إلكتروني، أو لأنها لا تفي بمتطلبات خدمة الإرسال الإلكتروني المضمون المؤهلة المنصوص عليها في المادة 28 أعلاه.

القسم الفرعي الخامس

التيقن من موقع الأنترنت

المادة 30

يتم التيقن من موقع الأنترنت من خلال شهادة مؤهلة للتيقن من الموقع المذكور.

وتسمح الشهادة الإلكترونية المذكورة بالتحقق من صدقية موقع الأنترنت، وربطه بالشخص الذاتي أو الاعتباري المسلمة إليه الشهادة. ولا يمكن تسليمها إلا من لدن مقدم خدمات ثقة معتمد.

المادة 31

تتضمن الشهادة المؤهلة للتيقن من موقع الأنترنت أصناف المعطيات المتعلقة :

- بمقدم خدمات الثقة المعتمد الذي سلم الشهادة المؤهلة ؛
- بالشخص الذاتي أو الاعتباري المسلمة إليه الشهادة، واسم أو أسماء المجال المستغل من لدن الشخص المذكور؛
- برمز تعريف الشهادة المؤهلة وصلاحيتها.

تحدد بنص تنظيمي قائمة أصناف المعطيات المذكورة.

الفرع الثاني

مقدمو خدمات الثقة

المادة 32

لا يمكن تقديم خدمة ثقة مؤهلة، وإصدار شهادات إلكترونية مؤهلة وتسليمها وتدبير العمليات المتعلقة بها، إلا من لدن مقدمي خدمات ثقة معتمدين وفق الشروط المحددة في هذا القانون والنصوص المتخذة لتطبيقه.

المادة 33

من أجل الحصول على الاعتماد، يجب على مقدم خدمات الثقة :

أولا - أن يستوفي الشروط التالية :

أ) أن يكون مؤسسا في شكل شركة خاضعة للقانون المغربي ؛

ب) أن يستعمل نظما ومعدات وبرمجيات موثوقا بها، ويضمن سلامتها التقنية وموثوقية سلسلة العمليات المتكفل بها ؛

ج) أن يوظف مستخدمين، وأن يلجأ عند الاقتضاء إلى مقاولين من الباطن، لهم التجربة والمؤهلات اللازمة في مجال تقديم خدمات الثقة ؛

د) أن يكتتب تأمينا لتغطية الأضرار التي يمكن أن تلحق كل شخص ذاتي أو اعتباري بسبب خطئه المهني ؛

هـ) أن يتوفر على مخطط لضمان استمرارية الخدمة، يتضمن مجموع الحلول البديلة لإبطال مفعول انقطاعات الأنشطة، وحماية الوظائف من الآثار الناجمة عن الاختلالات الأساسية للنظم أو عن الكوارث، وضمان استئناف عمل هذه الوظائف في أقرب الآجال.

ثانيا - أن يلتزم :

أ) بإخبار الشخص الذي يرغب في استعمال خدمة ثقة مؤهلة، إخبارا واضحا وشاملا، وقبل أي تعاقد معه، بالشروط المتعلقة باستعمال خدمة الثقة المذكورة، بما في ذلك حدود استعمالاتها ؛

ب) بالقدرة على المحافظة، عند الاقتضاء بشكل إلكتروني، على بعض المعطيات المتبادلة مع زبنائه لأجل تقديم خدمات الثقة، شريطة :

- ألا يسمح بإدخال المعطيات وتغييرها إلا للأشخاص المرخص لهم لهذا الغرض من لدن مقدم الخدمة ؛

- ألا يتأتى اطلاع العموم على المعطيات دون موافقة الزبون المعني المسبقة ؛

- أن يكون بالإمكان كشف أي تغيير من شأنه أن يخل بسلامة المعطيات.

علاوة على الشروط والالتزامات المنصوص عليها أعلاه، يجب على مقدم خدمات الثقة الذي يعتزم تسليم شهادات إلكترونية مؤهلة :

1 - أن يلتزم بالتحقق بوسائل ملائمة، من هوية الشخص الذاتي أو الاعتباري الذي يسلم له الشهادة الإلكترونية، وعند الاقتضاء، من جميع المعلومات الخاصة بالشخص المذكور. ويتم التحقق من هذه المعلومات :

أ) عن طريق الحضور الشخصي للشخص الذاتي أو للممثل المأذون له من لدن الشخص الاعتباري ؛

ب) أو عن بعد، بواسطة وسائل التعريف الإلكتروني التي تطلب تسليمها الحضور الشخصي للشخص الذاتي، أو للممثل المأذون له من لدن الشخص الاعتباري لدى الهيئة التي سلمت تلك الوسيلة. تحدد الوسائل المذكورة بنص تنظيمي ؛

ج) أو بواسطة شهادة إلكترونية مؤهلة للتوقيع الإلكتروني أو للخاتم الإلكتروني، التي سبق تسليمها لشخص تم التأكد من هويته وفق البندين (أ) أو (ب) من هذه الفقرة ؛

د) أو عن طريق وسائل أخرى للتعريف توفر ضمانة تعتبرها السلطة الوطنية معادلة للوسائل السالفة الذكر من حيث موثوقية الحضور الشخصي.

استثناء من أحكام المادة 32 أعلاه، يمكن التحقق من هذه المعلومات من قبل الغير، في إطار عقد مقاولة من الباطن يربط بين هذا الأخير ومقدم الخدمات المعني تصادق عليه السلطة الوطنية؛

2 - أن يسمح للشخص الذي سلمت له الشهادة الإلكترونية بإلغائها في الحال وبكل يقين، وأن يحرص على أن يتم تحديد تاريخ وساعة تسليم الشهادة الإلكترونية وتاريخ وساعة إلغائها بدقة، وأن ينشر وضعية الشهادة المذكورة فور إلغائها؛

3 - أن يقدم لكل طرف مستعمل المعلومات المتعلقة بصلاحية الشهادات المؤهلة التي سلمها أو وضعيات إلغائها، وأن يبقي هذه المعلومات متاحة في أي وقت وحين، حتى ما بعد مدة صلاحية الشهادات.

تحدد بنص تنظيمي كيفيات تطبيق هذه المادة.

المادة 34

استثناء من أحكام أ) من البند الأول من الفقرة الأولى بالمادة 33 أعلاه، ومع مراعاة مصلحة المرفق العام، يمكن للسلطة الوطنية اعتماد الأشخاص الاعتبارية الخاضعة للقانون العام من أجل تقديم خدمات الثقة وفق الشروط المنصوص عليها في هذا القانون والنصوص المتخذة لتطبيقه.

المادة 35

يتعين على كل شخص يرغب في تقديم خدمات ثقة لا تدخل ضمن الخدمات المؤهلة، التصريح مسبقا بذلك لدى السلطة الوطنية.

تحدد بنص تنظيمي كيفيات التصريح المسبق.

المادة 36

تتمتع خدمات الثقة المؤهلة المقدمة من قبل مقدم خدمات ثقة مستوطن بالخارج بنفس القيمة القانونية التي تتمتع بها الخدمات المؤهلة المقدمة من قبل مقدم خدمات ثقة يوجد مقره داخل التراب الوطني إذا كان معترفا بخدمة الثقة أو مقدم خدمة الثقة في إطار اتفاق متعدد الأطراف تعتبر المملكة المغربية طرفا فيه أو اتفاق ثنائي يتعلق بالاعتراف المتبادل بين المملكة وبلد إقامة مقدم الخدمات.

المادة 37

يتعين على مقدم خدمات ثقة قبل إنهاء أنشطته أن يخبر السلطة الوطنية مسبقا بذلك داخل أجل لا يقل عن شهرين.

وفي هذه الحالة، يجب عليه أن يتأكد من استئناف هذه الخدمات من لدن مقدم خدمات ثقة يضمن نفس المستوى من الجودة والسلامة أو، إذا تعذر ذلك، أن يلغي الشهادات داخل أجل أقصاه شهران بعد إخبار أصحابها بذلك.

يخبر مقدم الخدمات أيضا السلطة الوطنية، على الفور، بوقف نشاطه في حالة تصفية قضائية.

المادة 38

يلزم مقدمو خدمات الثقة ومستخدموهم بكتمان السر المهني، تحت طائلة العقوبات المنصوص عليها في التشريع الجاري به العمل. غير أنه لا يمكنهم الاحتجاج بكتمان السر المهني :

- تجاه السلطات الإدارية المؤهلة قانونا وفق التشريع الجاري به العمل ؛
- تجاه أعوان السلطة الوطنية، والخبراء المفوضين من لدنها والضباط المشار إليهم في المادة 59 بعده خلال ممارسة المهام المنصوص عليها في المواد 56 و59 و60 من هذا القانون ؛
- إذا وافق زبون مقدم خدمات ثقة على نشر المعلومات التي سبق أن أدلى بها إليه أو الاطلاع عليها.

المادة 39

يجب على مقدمي خدمات الثقة أن يقوموا بحفظ المعطيات المتعلقة بتقديم خدمة الثقة ويلزمون بتبليغها إلى السلطات القضائية، وذلك وفق الشروط المنصوص عليها في التشريع الجاري به العمل. وفي هذه الحالة، وعلى الرغم من كل المقتضيات التشريعية المخالفة، يتولى مقدمو خدمات الثقة إخبار الطرف المستعمل المعني على الفور بذلك.

المادة 40

يقوم مقدمو خدمات الثقة المعتمدون وغير المعتمدين بتبليغ السلطة الوطنية بكل مس بالسلامة أو فقدان التمامية، فور علمهم بذلك، والذي يترتب عليهما تأثير على خدمة الثقة المقدمة أو على المعطيات ذات الطابع الشخصي المحفوظة في هذه الخدمة.

عندما يكون من شأن المس بالسلامة أو فقدان التمامية، إلحاق ضرر بشخص ذاتي أو اعتباري قدمت له خدمة الثقة، يقوم مقدم خدمات الثقة بتبليغ ذلك فورا إلى الشخص المذكور.

الفرع الثالث

التزامات صاحب الشهادة الإلكترونية

المادة 41

يكون صاحب الشهادة الإلكترونية المؤهلة، فور إحداث المعطيات المرتبطة بإنشاء التوقيع الإلكتروني المؤهل أو الخاتم الإلكتروني المؤهل، مسؤولا وحده عن سرية وتمامية المعطيات المذكورة، عندما تكون هذه المعطيات موجودة في آليته المؤهلة لإنشاء التوقيع أو الخاتم المذكورين. ويعد كل استعمال لتلك المعطيات ناتجا عن فعله ما لم يثبت خلاف ذلك.

المادة 42

يجب على صاحب الشهادة الإلكترونية القيام في أقرب الآجال بتبليغ مقدم خدمات الثقة بكل تغيير يطرأ على المعلومات التي تتضمنها الشهادة المذكورة.

المادة 43

يجب على صاحب الشهادة أن يعمل على إلغائها فورا، في حالة الشك في الحفاظ على سرية المعطيات المتعلقة بإنشاء التوقيع الإلكتروني أو الخاتم الإلكتروني أو في حالة فقدان مطابقة المعلومات المضمنة في الشهادة للواقع.

المادة 44

عند انتهاء مدة صلاحية شهادة إلكترونية أو عند إلغائها، لا يمكن لصاحبها الاستمرار في استعمالها أو استعمال المعطيات المتعلقة بإنشاء التوقيع الإلكتروني أو الخاتم الإلكتروني المطابقة لهذه الشهادة قصد إنشاء توقيع إلكتروني أو خاتم إلكتروني أو الحصول على شهادة جديدة من لدن مقدم خدمات ثقة آخر على أساس المعطيات المذكورة.

الباب الثاني

وسائل وخدمات التشفير وتحليل الشفرات

المادة 45

تتجلى وسيلة التشفير وتحليل الشفرات في كل معدات أو برمجيات، مصممة أو معدلة من أجل تحويل معطيات إلكترونية سواء كانت عبارة عن معلومات أو إشارات أو رموز استنادا إلى اتفاقيات سرية، أو من أجل إنجاز العملية العكسية، بموجب اتفاقية سرية أو بدونها.

وتهدف وسيلة التشفير وتحليل الشفرات على الخصوص إلى ضمان سلامة تبادل المعطيات بطريقة إلكترونية أو تخزينها، بكيفية تمكن من ضمان سريتها والتيقن منها ومراقبة تماميتها.

خدمة التشفير وتحليل الشفرات هي كل عملية تهدف إلى توظيف وسائل التشفير وتحليل الشفرات لحساب الغير.

المادة 46

من أجل الحفاظ على مصالح الدفاع الوطني وأمن الدولة، يخضع استيراد وسائل التشفير وتحليل الشفرات أو تصديرها أو توريدها وكذا تقديم خدمات التشفير وتحليل الشفرات :

أ) لتصريح مسبق لدى السلطة الوطنية عندما ينحصر الغرض من هذه الوسيلة أو هذه الخدمة في التيقن من إرسالية أو ضمان تمامية المعطيات المرسلة بطريقة إلكترونية؛

ب) لترخيص من قبل السلطة الوطنية عندما يتعلق الأمر بغرض غير الغرض المشار إليه في البند أ) أعلاه.

تحدد بنص تنظيمي كيفيات الإدلاء بالتصريح وتسليم الترخيص.

تعفى من التصريح والترخيص المذكورين بعض أنواع وسائل أو خدمات التشفير وتحليل الشفرات التي تحدد قائمتها بنص تنظيمي.

لا تخضع الأجهزة المكلفة بالدفاع الوطني وبأمن الدولة لنظامي التصريح والترخيص المنصوص عليهما في هذه المادة.

المادة 47

يودع التصريح المسبق المنصوص عليه في المادة 46 أعلاه، مقابل وصل بالتسلم، ثلاثين (30) يوما على الأقل قبل التاريخ المحدد لإنجاز العملية المعنية بهذا التصريح.

يجب إخبار السلطة الوطنية بكل تغيير يطرأ على أحد العناصر التي تم على أساسها الإدلاء بالتصريح داخل أجل لا يتعدى ثمانية (8) أيام من حدوثه.

المادة 48

يتضمن الترخيص المنصوص عليه في المادة 46 أعلاه، البيانات التي تمكن من التعرف على صاحبه، ورقم الترخيص وتاريخ تسليمه ومدة صلاحيته، وكذا الوسائل أو الخدمات التي سلم من أجلها.

لا يمكن أن تتجاوز مدة الترخيص خمس (5) سنوات.

يجب إخبار السلطة الوطنية بكل تغيير يطرأ على أحد العناصر التي تم على أساسها تسليم الترخيص داخل أجل لا يتعدى ثمانية (8) أيام من حدوثه.

المادة 49

يمكن إيقاف الترخيص لمدة لا تتعدى ثلاثة (3) أشهر في حالة تغيير المتطلبات التي تم على أساسها تسليم الترخيص المذكور.

المادة 50

يسحب الترخيص في الحالات التالية :

- تقديم معلومات خاطئة من أجل الحصول على الترخيص ؛
- عدم تقيد صاحب الترخيص بأحكام هذا القانون والنصوص المتخذة لتطبيقه ؛
- عدم تقيد صاحب الترخيص، إثر اتخاذ مقرر بالإيقاف، بالمتطلبات المبينة في المقرر المذكور ؛
- توقف صاحب الترخيص عن ممارسة النشاط المرخص له به.

المادة 51

يكون مقدمو خدمات التشفير وتحليل الشفرات لأغراض سرية مسؤولين، فيما يخص هذه الخدمات، عن الضرر اللاحق بالأشخاص الذين كلفوهم بتدبير اتفاقياتهم السرية، في حالة المس بتمامية المعطيات المحولة بواسطة هذه الاتفاقيات أو بسريتها أو بتوفرها، ما لم يثبتوا عدم ارتكابهم أي خطأ متعمد أو تهاون.

الباب الثالث

السلطة الوطنية لخدمات الثقة بشأن المعاملات الإلكترونية

المادة 52

يعهد إلى السلطة الوطنية لخدمات الثقة بشأن المعاملات الإلكترونية، علاوة على الاختصاصات المسندة إليها بموجب مواد أخرى من هذا القانون، بالمهام التالية :

- تحديد المعايير والدلائل المرجعية المطبقة على خدمات الثقة المذكورة، واتخاذ التدابير اللازمة لتنفيذها ؛
- اعتماد مقدمي خدمات الثقة المؤهلة ومراقبة أنشطتهم ؛
- المراقبة البعدية لمقدمي خدمات الثقة غير المعتمدين ؛
- اقتراح مشاريع النصوص التشريعية والتنظيمية المتعلقة بخدمات الثقة بشأن المعاملات الإلكترونية.

المادة 53

تقوم السلطة الوطنية بنشر مستخرج من مقرر الاعتماد بالجريدة الرسمية، وبمسك سجل مقدمي خدمات الثقة المعتمدين ينشر في نهاية كل سنة بالجريدة الرسمية.

تنشر السلطة الوطنية بموقع الأنترنت الخاص بها لائحة مقدمي خدمات الثقة المعتمدين ولائحة مقدمي الخدمات غير المعتمدين الذين قدموا تصريحهم المسبق المنصوص عليه في المادة 35 من هذا القانون.

المادة 54

تتحقق السلطة الوطنية من مدى احترام مقدمي خدمات الثقة للالتزامات المنصوص عليها في أحكام هذا القانون والنصوص المتخذة لتطبيقه.

المادة 55

يمكن للسلطة الوطنية، إما تلقائيا وإما بطلب من أي شخص يهمه الأمر، أن تراقب أو أن تعمل على مراقبة مطابقة أنشطة مقدم خدمات الثقة لأحكام هذا القانون والنصوص المتخذة لتطبيقه. ويمكنها أن تستعين بخبراء لإنجاز مهامها المتعلقة بالمراقبة.

يتحمل مقدم خدمات الثقة التكاليف المتعلقة بالمراقبة.

المادة 56

يخول أعوان السلطة الوطنية وكذا الخبراء المفوضون من لدنها، خلال ممارسة مهمة المراقبة المكلفين بها المنصوص عليها في المادة 55 أعلاه، بعد إثبات صفتهم، حق الولوج إلى أي مؤسسة والاطلاع على كل الآليات والوسائل التقنية المتعلقة بخدمات الثقة والتي يعتبرونها مفيدة أو ضرورية لإنجاز مهمتهم.

ينجز الأعوان بعد انتهاء مهمة المراقبة المذكورة، تقريرا تستند إليه السلطة الوطنية، عند الاقتضاء، لاتخاذ التدابير المنصوص عليها في المادة 61 أدناه.

المادة 57

يلزم أعوان السلطة الوطنية والخبراء المنصوص عليهم في المادة 56 أعلاه بكتمان السر المهني، تحت طائلة العقوبات المنصوص عليها في مجموعة القانون الجنائي فيما يخص جميع المعلومات التي يطلعون عليها بمناسبة القيام بمهمة المراقبة.

المادة 58

إذا كان من شأن أنشطة مقدم خدمات الثقة أن تمس بمتطلبات الدفاع الوطني أو أمن الدولة، تؤهل السلطة الوطنية لاتخاذ جميع التدابير التحفظية الضرورية لوضع حد للأنشطة المذكورة، دون الإخلال بالمتابعات الجنائية التي تترتب عليها.

الباب الرابع

البحث عن المخالفات ومعاينتها والعقوبات المطبقة عليها

المادة 59

علاوة على ضباط الشرطة القضائية وأعوان إدارة الجمارك والضرائب غير المباشرة العاملين وفق اختصاصاتهم، يؤهل أعوان السلطة الوطنية المفوضون لهذا الغرض والمحلفون وفق التشريع الجاري به العمل، للبحث عن المخالفات لأحكام هذا القانون والنصوص المتخذة لتطبيقه ومعاينتها بواسطة محاضر.

تحال محاضر معاينة المخالفات إلى النيابة العامة المختصة داخل أجل أقصاه ثمانية (8) أيام ابتداء من تاريخ إنجازها.

المادة 60

علاوة على الاختصاصات المخولة لأعوان السلطة الوطنية برسم مهام المراقبة المنصوص عليها في المادة 55 أعلاه، يمكن لهؤلاء الأعوان كذلك الولوج إلى الأماكن أو الأراضي أو وسائل النقل المعدة لغرض مهني وطلب الاطلاع على كل الوثائق المهنية وأخذ نسخ منها والحصول على المعلومات والإثباتات بعد استدعاء المعنيين بالأمر أو بعين المكان.

ويجوز لهم حجز كل منتوج أو مادة أو وثيقة أو وسيلة نقل لها صلة بالمخالفة التي تمت معاينتها. وتكون كل المنتوجات أو المواد أو الوثائق أو وسائل النقل التي تم حجزها موضوع جرد يلحق بمحضر معاينة المخالفة.

المادة 61

عندما يتبين للسلطة الوطنية، بناء على تقرير أعوانها، أن مقدم خدمات الثقة المعتمد لم يعد يستوفي أحد الشروط المنصوص عليها في المادة 33 من هذا القانون أو أن نشاطه غير مطابق لأحكام هذا القانون أو النصوص المتخذة لتطبيقه، فإنها توجه إليه إعذارا من أجل التقيد بالشروط أو بالأحكام المذكورة داخل الأجل الذي تحدده.

إذا لم يستجب مقدم الخدمات للإعذار بعد انصرام الأجل المذكور، تقوم السلطة الوطنية بسحب الاعتماد، وبالتشطيب على مقدم الخدمات من سجل مقدمي الخدمات المعتمدين، وبنشر مستخرج من مقرر سحب الاعتماد بالجريدة الرسمية.

المادة 62

يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 100.000 إلى 500.000 درهم كل من قدم خدمات ثقة مؤهلة دون أن يكون معتمدا طبقا لأحكام المادة 33 من هذا القانون أو واصل نشاطه رغم سحب اعتماده أو أصدر أو سلم أو دبر شهادات إلكترونية مؤهلة خرقا لأحكام المادة 32 من نفس القانون.

المادة 63

يعاقب بغرامة من 50.000 إلى 100.000 درهم، كل من قدم خدمة ثقة لا تدخل ضمن خدمات الثقة المؤهلة، دون القيام بالتصريح المنصوص عليه في المادة 35 من هذا القانون.

المادة 64

دون الإخلال بالعقوبات الجنائية الأشد المنصوص عليها في التشريع الجاري به العمل، يعاقب بالحبس من شهر إلى ستة أشهر وبغرامة من 20.000 إلى 50.000 درهم، كل مقدم خدمة ثقة أو أحد مستخدميه أفشى المعلومات المعهود بها إليه في إطار ممارسة أنشطته أو وظائفه أو حرض على إفشائها أو ساهم في ذلك، خرقا لأحكام المادة 38 من هذا القانون.

المادة 65

دون الإخلال بالعقوبات الجنائية الأشد المنصوص عليها في التشريع الجاري به العمل، يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 100.000 إلى 500.000 درهم، كل من أدلى عمدا بتصريحات كاذبة أو سلم وثائق مزورة إلى مقدم خدمات الثقة من أجل الحصول على خدمة ثقة.

المادة 66

دون الإخلال بالعقوبات الجنائية الأشد المنصوص عليها في التشريع الجاري به العمل، يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 إلى 100.000 درهم، كل من قام باستيراد أو تصدير أو تقديم إحدى وسائل التشفير وتحليل الشفرات أو خدمة من خدماتها دون القيام بالتصريح أو الحصول على الترخيص المنصوص عليهما في المادة 46 من هذا القانون.

علاوة على ذلك، يجوز للمحكمة أن تحكم بمصادرة وسائل التشفير وتحليل الشفرات المعنية.

ويعاقب بالحبس من شهر إلى ستة أشهر وبغرامة من 50.000 إلى 100.000 درهم، المصرح أو صاحب الترخيص الذي أخل بواجب إخبار السلطة الوطنية بكل تغيير طرأ على أحد العناصر التي تم على أساسها الإدلاء بالتصريح أو تسليم الترخيص المنصوص عليهما في المادة 46 من هذا القانون.

المادة 67

عندما يتم استعمال وسيلة للتشفير وتحليل الشفرات، لإعداد أو ارتكاب جناية أو جنحة أو لتسهيل إعدادها أو ارتكابها، يرفع الحد الأقصى للعقوبة السالبة للحرية المتعرض لها على النحو التالي :

- إلى السجن المؤبد إذا كانت الجريمة معاقبا عليها بالسجن بثلاثين سنة ؛
- إلى السجن بثلاثين سنة إذا كانت الجريمة معاقبا عليها بالسجن بعشرين سنة ؛

- إلى السجن بعشرين سنة إذا كانت الجريمة معاقبا عليها بالسجن بخمس عشرة سنة ؛
- إلى السجن بخمس عشرة سنة إذا كانت الجريمة معاقبا عليها بالسجن بعشر سنوات ؛
- إلى السجن بعشر سنوات إذا كانت الجريمة معاقبا عليها بالسجن بخمس سنوات ؛
- إلى الضعف إذا كانت الجريمة معاقبا عليها بالحبس بثلاث سنوات على الأكثر.

غير أن أحكام هذه المادة لا تطبق على مرتكب الجريمة أو المساهم أو المشارك في ارتكابها الذي يسلم إلى السلطات القضائية أو الإدارية، بطلب منها، النص الواضح للرسائل المشفرة وكذا الاتفاقيات السرية اللازمة لقراءة النص المشفر.

المادة 68

يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 10.000 إلى 100.000 درهم، كل من استعمل، بوجه غير قانوني، معطيات إنشاء التوقيع الإلكتروني أو إنشاء الخاتم الإلكتروني التي تخص الغير.

المادة 69

يعاقب بالحبس من ثلاثة إلى ستة أشهر وبغرامة من 10.000 إلى 100.000 درهم، كل مقدم خدمات الثقة الذي لا يتقيد بواجب إخبار السلطة الوطنية المنصوص عليه في المادة 37 من هذا القانون.

المادة 70

يعاقب بغرامة من 50.000 إلى 100.000 درهم، كل مقدم خدمة ثقة :

- لم يتقيد بواجب تبليغ السلطة الوطنية المنصوص عليه في المادة 40 من هذا القانون ؛
- لم يقم بحفظ المعطيات المتعلقة بتقديم خدمة الثقة، أو لم يقم بتبليغها إلى السلطات القضائية، أو لم يقم بإخبار الطرف المستعمل بذلك، وفقا لأحكام المادة 39 من هذا القانون، وذلك دون الإخلال بالعقوبات الجنائية الأشد.

المادة 71

يعاقب بالحبس من ستة أشهر إلى سنتين وبغرامة من 10.000 إلى 100.000 درهم، كل صاحب شهادة إلكترونية انتهت مدة صلاحيتها أو تم إلغاؤها، استمر في استعمال هذه الشهادة أو في استعمال المعطيات المتعلقة بإنشاء التوقيع الإلكتروني أو الخاتم الإلكتروني المطابقة لهذه الشهادة، وذلك خرقا لأحكام المادة 44 من هذا القانون.

المادة 72

دون الإخلال بالعقوبات الجنائية الأشد المنصوص عليها في التشريع الجاري به العمل، يعاقب بغرامة من 50.000 إلى 500.000 درهم كل من استعمل بصفة غير قانونية عنوانا تجاريا أو إشهارا وبشكل عام كل عبارة تحمل على الاعتقاد أنه معتمد لتقديم خدمة ثقة دون استيفائه للشروط المنصوص عليها في المادة 33 من هذا القانون.

المادة 73

إذا كان مرتكب الجريمة شخصا معنويا، ترفع الغرامات المنصوص عليها في هذا القانون إلى الضعف، دون الإخلال بالعقوبات التي يمكن تطبيقها على مسيريه المسؤولين على ارتكاب إحدى الجرائم المنصوص عليها في نفس القانون.

المادة 74

في حالة العود، ترفع العقوبات المنصوص عليها في هذا القانون إلى الضعف.

يعتبر في حالة العود، كل من سبق الحكم عليه بعقوبة من أجل ارتكاب إحدى المخالفات المنصوص عليها في هذا القانون بمقرر قضائي مكتسب لقوة الشيء المقضي به، ثم ارتكب نفس المخالفة قبل مضي أربع (4) سنوات من تمام تنفيذ تلك العقوبة أو تقادمها.

لتقرير حالة العود، تعتبر بمثابة نفس المخالفة جميع المخالفات المنصوص عليها في هذا القانون.

المادة 75

يمكن أن تطبق أيضا على الأشخاص الذين ثبتت مسؤوليتهم عن إحدى المخالفات المنصوص عليها أعلاه العقوبات الإضافية والتدابير الوقائية المنصوص عليها في مجموعة القانون الجنائي.

القسم الثاني

أحكام بتغيير قانون الالتزامات والعقود

المادة 76

تغير على النحو التالي أحكام الفصلين 2.1 (الفقرة 3) و3-417 (الفقرة 3) من الظهير الشريف بمثابة قانون الالتزامات والعقود، الصادر في 9 رمضان 1331 (12 أغسطس 1913) :

«الفصل 2.1 (الفقرة 3). - غير أن الوثائق المتعلقة بتطبيق .....
«من لدن شخص لأغراض مهنته، والمحررات المنجزة من لدن مؤسسات
«الائتمان والهيئات المعتبرة في حكمها.»

«الفصل 3-417 (الفقرة 3). - تتمتع كل وثيقة مذيلة بتوقيع إلكتروني
«مؤهل وبختم زمني إلكتروني مؤهل بنفس قوة .....
«بتاريخ ثابت.»

المادة 77

تحل عبارة «مؤهل» محل عبارة «مؤمن» الواردة في الفصول 3-417 (الفقرتان الأولى والثانية) و425 و426 من الظهير الشريف بمثابة قانون الالتزامات والعقود.

القسم الثالث

أحكام مختلفة وانتقالية وختامية

المادة 78

تحدد بنص تنظيمي قيمة الضمانات الشخصية أو العينية موضوع المحررات المنجزة من لدن مؤسسات الائتمان والمؤسسات المعتبرة في حكمها، المنصوص عليها في الفصل 2.1 من قانون الالتزامات والعقود، التي يستعمل فيها وجوبا التوقيع الإلكتروني المتقدم أو المؤهل أو الخاتم الإلكتروني المتقدم أو المؤهل.

المادة 79

تحدد كيفيات تطبيق أحكام هذا القانون على الحقوق العينية بنص تنظيمي.

المادة 80

يجب على مقدم خدمات المصادقة الإلكترونية المعتمد الذي يقوم، في تاريخ دخول هذا القانون حيز التنفيذ، بتسليم شهادات مؤمنة وفقا لأحكام القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، أن يتقيد بأحكام هذا القانون داخل أجل سنة ابتداء من تاريخ دخوله حيز التنفيذ.

المادة 81

تظل شهادة المطابقة لآلية إنشاء التوقيع الإلكتروني، المسلمة وفقا لأحكام القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، سارية المفعول مادامت هذه الآلية تستجيب لمتطلبات هذا القانون.

المادة 82

تعتبر الشهادات الإلكترونية المؤمنة المسلمة وفقا لأحكام القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، بمثابة شهادات إلكترونية مؤهلة حسب أحكام هذا القانون، إلى حين انتهاء صلاحيتها.

المادة 83

ينسخ الباب التمهيدي والقسم الثاني من القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية الصادر بتنفيذه الظهير الشريف رقم 1.07.129 بتاريخ 19 من ذي القعدة 1428 (30 نوفمبر 2007).

المادة 84

يدخل هذا القانون حيز التنفيذ ابتداء من تاريخ نشر النصوص المتخذة لتطبيقه بالجريدة الرسمية.

ملخص تدخلات السيدات والسادة المستشارين

لقد شكلت المناقشة العامة فرصة أجمع من خلالها كافة المتدخلين على قيمة وأهمية هذا المشروع قانون ودلالاته العلمية والتقنية الرامية إلى سن نظام أكثر شمولية يسمح برقمنة غالبية المعاملات الإلكترونية، وإضفاء مرونة أكبر في الاعتماد الواسع على المصادقة الإلكترونية، وتحديد مستويات مختلفة للتوقيع الإلكتروني تتلاءم ونوعية المعاملات الإلكترونية ، مما يشكل دفعة جديدة لجاذبية بلادنا ومصداقيتها وتنافسيتها على الصعيد الدولي في مجالات التحول الرقمي، ومن جهة أخرى أكد السيدات والسادة المستشارون أن هذا المشروع قانون يأتي في سياق دولي متميز لبلادنا بفضل القرار التاريخي للولايات المتحدة الأمريكية الذي تم من خلاله الاعتراف بسيادة المغرب على كامل تراب الصحراء المغربية، والدينامية الجديدة المتمثلة في فتح البعثات والقنصليات الدبلوماسية بمدينتي العيون والداخلة مما كرس عزلة خصوم الوحدة الترابية، هذا فضلا عن التدخل الحكيم لقوات المسلحة الملكية في تأمين معبر الكركرات بفضل القيادة الرشيدة لصاحب الجلالة الملك محمد السادس القائد الأعلى ورئيس أركان الحرب العامة، الشيء الذي كرس من جديد أجواء المسيرة الخضراء المظفرة وعزز الإجماع الوطني.

ونظرا للحمولة التقنية لهذا المشروع قانون ومقتضياته الجديدة تمت الدعوة إلى :

- ضبط المفاهيم والمرتكزات والوظائف الجديدة التي بموجبها سيتم تكريس الثقة بشأن المعاملات الإلكترونية ؛
- مصداقية والتزامات مقدمي خدمات الثقة وإثبات الصحة في مجال المعاملات الإلكترونية وفق دفتر تحملات واضح المعالم ؛
- تعزيز البنية التحتية : صبيب الإنترنت، والشبكة الكهربائية ؛
- ضمان الأمن السيبراني في كافة المعاملات الإلكترونية ؛
- إعمال مبدأ التدرج في منح الشهادات والختم الزمني والإرسال الإلكتروني المضمون؛
- تعزيز التعاون والشراكة مع الاتحاد الأوروبي (فرنسا وإسبانيا كنموذج) وباقي الشركاء ؛
- تعزيز الانفتاح العلمي والتقني على مراكز البحوث والجامعات والاهتمام بمجال البيئة الرقمية وشهادات البراءة ؛
- تنزيل النصوص التنظيمية في أقرب الآجال لمواكبة التطبيق السليم لهذا القانون في أبعاده الاقتصادية والاجتماعية والمجالية ؛
- تبسيط المساطر والمعاملات الإلكترونية ولاسيما فيما يخص دعم التحول الرقمي بالنسبة للمقاولات الصغيرة والمتوسطة وباقي المتعاملين؛

- تأهيل الموارد البشرية وإعادة النظر في منظومة التعليم والتكوين والتشغيل لتفادي إشكال هجرة الكفاءات ؛
- الاعتناء بالتجارة الإلكترونية على غرار التجربة الجديدة لغرف التجارة والصناعة والخدمات ؛
- التفكير المستقبلي في إدراج الاقتصاد غير المهيكل في المنظومة الرقمية؛
- توفير الضمانات الأمنية والقانونية لحماية المتعاملين إلكترونيا من خلال سن تشريعات صارمة في هذا المجال ؛
- تكوين قضاة متخصصين في المجال التكنولوجي والرقمي لمواكبة هذه الدينامية ؛
- إعطاء الحجية القانونية للتوقيع الإلكتروني وأثره القانوني أمام القضاء وإضفاء مرونة أكبر في الاعتماد الواسع على المصادقة الإلكترونية ؛

ومن جهة أخرى أشار أحد المتدخلين لغياب التواصل قبل الشروع في مسطرة المصادقة على هذا النص ، وفي هذا الإطار أشار لضرورة تنظيم أيام

دراسية وورشات داخل المؤسسة التشريعية لبسط مضامينه ومقتضياته القانونية قبل المصادقة عليه والشروع في تنزيله.

وفي السياق ذاته استأثر النقاش بجملة من الاستفسارات والتساؤلات همت بالخصوص :

- دور السلطة الوطنية ومجالات اختصاصاتها والتعيين بها وكذا علاقتها بمقدمي خدمات الثقة وإثبات الصحة في مجال المعاملات الإلكترونية؛
- الفرق بين التوقيع الإلكتروني والتوقيع البيومتري ؛
- الأثر السلبي للمعاملات التقليدية السارية في مواكبة التحول الرقمي الجديد ؛
- إشكالية الثقة بالمعاملات الإلكترونية بين الفاعلين والشركاء والمتعهدين من حيث حماية المعطيات الشخصية والمعاملات الرقمية ؛
- غياب تبسيط بعض المقتضيات القانونية الواردة في النص التي من شأنها فك كل التباس أو تفسير ولاسيما بعض المواد على سبيل المثال:

المادة 55 -- المادة 60 -- المادة 76 -- المادة 79-- المادة 83

- طبيعة العلاقة بين المشروع قانون 43.20 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية والقانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية ؛
- دور هذا القانون في حماية الحقوق العينية ؛
- تحديد الاختصاصات في مجال التنظيم ومجال التشريع احتراما لمبدأ فصل السلط ؛
- حجية التوقيع الإلكتروني كوسيلة إثبات ومدى أهمية الضمانات التي يوفرها للمتعاملين بغية حمايتهم من التزوير.

جواب السيد الوزير

المملكـــــة المغـــربية

إدارة الدفاع الوطني

جواب السيد الوزير المنتدب لدى رئيس الحكومة المكلف بإدارة الدفاع الوطني بشأن مداخلات السيدات والسادة المستشارين أثناء مناقشة مشروع القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الالكترونية.

السيد رئيس اللجنة المحترم،

السيدات والسادة المستشارين المحترمين،

أود في البداية أن أجدد لكم شكري وامتناني وتقديري لما تولونه من اهتمام بالغ ودعم متواصل لمقترحات ومبادرات إدارة الدفاع الوطني سواء أثناء مناقشة مشاريع القوانين التي تخص هذا القطاع أو من خلال دراسة ومناقشة الميزانية الفرعية لهذه الإدارة في إطار المصادقة على قانون المالية لكل سنة.

وإذ أشيد بالمناقشة الغنية والهادفة التي ميزت هذا الاجتماع، يسعدني، أن أضع بين أيديكم بعض التوضيحات والأجوبة، تفاعلا مع مختلف الأسئلة التي تفضلتم بطرحها، وذلك من خلال المحاور التالية:

- تقييم التجربة التي راكمتها بلادنا في مجال المصادقة الالكترونية؛
- النصوص التطبيقية لمشروع هذا القانون؛
- السلطة الوطنية لخدمات الثقة بشأن المعاملات الإلكترونية؛
- المقتضيات ذات الطابع الزجري في مشروع هذا القانون؛
- استعمال اسم مستعار أثناء التوقيع؛
- خدمة الإرسال الإلكتروني المضمون وعلاقته بالتوقيع الالكتروني؛
- العلاقة بين وسائل وخدمات التشفير وخدمات الثقة؛
- دور إدارة الدفاع الوطني في تعزيز الثقة الرقمية؛
- مواكبة تطبيق القانون والحملات التحسيسية.

المحور الأول: تقييم التجربة التي راكمتها بلادنا في مجال المصادقة الالكترونية

1

يعتبر القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية أول إطار قانوني لاستعمال المصادقة الإلكترونية تم اعتماده ببلادنا سنة 2007، إلا أنه وبالرغم من التغيرات السريعة التي يعرفها مجال المعاملات الالكترونية، وعلى مر 13 سنة من تطبيق هذا القانون راكمت بلادنا تجربة متواضعة في هذا المجال.

وفي إطار تقييم هذه التجربة ومحاولة إغنائها، اتضح جليا أن هذا القانون لم يكن مرنا بالشكل الذي يسمح بتطوير شامل للمصادقة الإلكترونية، حيث اقتصرت المصادقة الإلكترونية على خدمة التوقيع الإلكتروني فقط، ومن أجل تجاوز هذا الوضع، ظهرت العديد من المؤشرات التي شجعت على إعادة النظر في التشريع الحالي وجعله مواكبا ومتماشيا مع التطورات التكنولوجية العالمية. ومن بين هذه المؤشرات ما يلي:

- ✓ لم يرق التصديق الالكتروني في بلادنا إلى مستوى التطلعات حيث لم يتجاوز عدد الشهادات الإلكترونية المسلمة، منذ دخول هذا القانون حيز التنفيذ وإلى غاية اليوم، 25.000 شهادة غالبيتها تتعلق بالتيقن (authentification) والتي تسمح بتأكيد التعريف الإلكتروني لشخص ذاتي أو اعتباري؛
- ✓ نطاق استعمالات الشهادات الإلكترونية الحالية جد محدود ولم يتم بالشكل الكافي التأطير القانوني للتوقيع الالكتروني البسيط عكس التوقيع الالكتروني المؤمن، مما حمل على الاعتقاد بأنه غير مؤمن، مع العلم أن هذا التوقيع يفي لمتطلبات حاجيات مختلف الإدارات والمؤسسات وكذا الفاعلين الاقتصاديين التي عبروا عنها خلال مجموعة من الاجتماعات التي نظمتها المديرية العامة لأمن نظم المعلومات في إطار التحضير ودراسة مسودة مشروع هذا القانون؛
- ✓ غياب مشاريع رقمية كبرى تستدعي اللجوء إلى التوقيع الإلكتروني، التي كان من شأنها أن تخلق تنافسية وبالتالي فتح المجال لاستقطاب مقدمين آخرين لخدمات المصادقة الالكترونية، والتي تقتصر منذ دخول القانون حيز التطبيق على مقدم خدمة معتمد وحيد؛
- ✓ جمع مقترحات الفاعلين في مجال المصادقة الالكترونية ودراستها مع الاستئناس بالتجارب الدولية، حيث استغرقت الدراسة والتحضير لمشروع هذا القانون سنتين اعتبارا للأهمية التي يكتسيها تنظيم هذا الموضوع.

المحور الثاني: النصوص التطبيقية لمشروع هذا القانون

تعتبر النصوص التنظيمية من الآليات التي تساهم في التطبيق السليم للنصوص القانونية، إذ لا يمكن للقانون الإحاطة والتفصيل في جميع الأحكام التي ستؤطر الموضوع، وفي هذا الإطار أحال مشروع القانون 43.02 في مجموعة من مقتضياته، كما هو الحال بالنسبة للقانون 53.05، على نصوص تنظيمية من أجل تحديد شروط التنفيذ وتفصيلات المبادئ العامة التي أقرها.

لقد تمت صياغة مشروع هذا القانون بشكل جعله مستوعبا لجميع الملاحظات والتصور الشمولي الذي أفرزته الممارسة والدراسات والمشاورات المنجزة حول هذا الموضوع، وذلك وفق هيكلة جديدة، مع الالتزام في نفس الوقت بالدقة ومراعاة نوعية الأحكام التي تضمنها والمتسمة بالتغيرات التي يعرفها الفضاء الرقمي والتكنولوجي.

واعتبارا لخاصية التطور التي تميز موضوع مشروع هذا القانون كان لابد من الإحالة على نصوص تنظيمية تسمح بالأخذ بعين الاعتبار هذه الظروف.

وكما جرت العادة، فإن إدارة الدفاع الوطني تعمل بالموازاة مع إعداد مشاريع القوانين على البدء في إعداد النصوص التنظيمية لهذه القوانين، وتأتي هذه الخطوة الاستباقية وعيا من إدارة الدفاع الوطني بأهمية إصدار النصوص التنظيمية التي تجعل القانون الموافق عليه من طرف السلطة التشريعية يدخل حيز التنفيذ بشكل تام بعد أشهر قليلة من صدوره في الجريدة الرسمية، وبالتالي منحه القوة اللازمة، مع العلم أنه لم يسجل أي تأخر أو تباطؤ من هذه الإدارة في إصدار النصوص التطبيقية.

المحور الثالث: السلطة الوطنية لخدمات الثقة بشأن المعاملات الإلكترونية

تماشيا مع مقتضيات هذا القانون، تختص السلطة الوطنية بتنزيل هذه الإجراءات على أرض الواقع من خلال المهام التي أنيطت بها، على غرار السلطة الوطنية المنصوص عليها في المادة 15 من القانون الحالي رقم 53.05، مع تحيين هذه المهام تماشيا مع مستجدات مشروع نص هذا القانون.

وفي هذا الإطار، أوكل مشروع هذا القانون إلى السلطة الوطنية لخدمات الثقة بشأن المعاملات الإلكترونية بعض الاختصاصات ذات **الطابع الإداري والتنظيمي**، من أجل ممارسة المهام التالية:

- تحديد المعايير والدلائل المرجعية المطبقة على خدمات الثقة؛
- اعتماد مقدمي خدمات الثقة المؤهلة؛
- الترخيص أو تلقي التصاريح المسبقة، حسب الحالة، بشأن استيراد وسائل التشفير وتحليل الشفرات أو تصديرها أو توريدها؛
- مراقبة مقدمي خدمات الثقة؛
- اقتراح مشاريع النصوص التشريعية والتنظيمية المتعلقة بخدمات الثقة بشأن المعاملات الإلكترونية.

ومن خلال هذه الاختصاصات، يتضح أن الأمر لا يستدعي إحداث وكالة بهذا الخصوص، حيث أن جل المهام الموكولة لهذه السلطة لها طابع إداري وتنظيمي.

المحور الرابع: المقتضيات ذات الطابع الزجري في مشروع هذا القانون

لضمان **التطبيق الفعال** لأحكام مشروع هذا القانون نص على مجموعة من العقوبات والغرامات لمواجهة كل إخلال بمقتضياته. ولما كان من الضروري سن هذه المقتضيات الزجرية لضمان الالتزام والتطبيق الصارم للقانون، فإنه تم الحرص على مراعاة انسجامها مع السياسة الجنائية المعتمدة في بلادنا.

وهكذا، خصص الباب الرابع من القسم الأول من مشروع هذا القانون "للبحث عن المخالفات ومعاينتها والعقوبات المطبقة عليها"، وذلك عبر مواد تضمنت عقوبات وغرامات مالية مماثلة لتلك المنصوص عليها في القانون

الحالي رقم 53.05. غير أن هذا لا يتعارض مع الطابع المرن الذي يتسم به تطبيق مقتضيات مشروع هذا القانون، حيث لم يتم اللجوء إلى الأحكام الزجرية إلا في الحالات الضرورية والتي تقتضي سن عقوبات لضمان الامتثال لبعض الالتزامات.

المحور الخامس: استعمال اسم مستعار أثناء التوقيع

سمح مشروع هذا القانون، على غرار القانون 53.05 وكذا التشريعات الدولية المقارنة، للموقع صاحب الشهادة الالكترونية بإدراج اسم مستعار في الشهادة بدل اسمه الحقيقي.

واعتبار لكون الاسم المستعار هو اسم يطلقه الموقع على نفسه، وضع مشروع القانون، وفقا للمادة 39، على عاتق مقدمي خدمات الثقة التزام حفظ المعلومات التي تسمح بتحديد الهوية الحقيقية للموقع وإبلاغها عند الطلب وطبقا للقانون إلى السلطات القضائية.

أولا: الحق في استخدام اسم مستعار

إذا كان مشروع هذا القانون قد أجاز للموقع، **عند الاقتضاء**، وضع اسم مستعار في الشهادة بدل اسمه الحقيقي، فإن ذلك لا يعتبر قاعدة عامة بل استثناء.

وفي هذا الإطار، خولت المادة 2 من مشروع هذا القانون للموقع الحق في الحصول على شهادة للتوقيع الإلكتروني باسم مستعار بدل هويته الحقيقية، وذلك من خلال تعريف هذه المادة **لشهادة التوقيع الإلكتروني** على النحو الآتي: شهادة إلكترونية تربط معطيات إثبات صحة التوقيع الإلكتروني بشخص ذاتي، والتي تؤكد اسم الشخص المذكور أو **اسمه المستعار عند الاقتضاء**.

وفي المقابل، اشترطت المادة 10 من أجل تأكيد عملية إثبات صحة توقيع إلكتروني مؤهل صحة هذا التوقيع، مجموعة من الشروط من بينها أن يتم، في حالة استعمال اسم مستعار أثناء التوقيع، إخبار الطرف المستعمل بذلك بشكل واضح. فالموقع الذي لا يرغب في كشف هويته الحقيقية، يمكنه اختيار اسم مستعار.

ثانيا: شروط استخدام أسم مستعار

نص المشروع على شرطين لاستخدام اسم مستعار في شهادة التوقيع الالكترونية من قبل مقدمي خدمات الثقة:

- التعريف بالاسم المستعار بهذه الصفة: حيث تلزم المادة 10 مقدم خدمات الثقة بأن يشير في الشهادة إلى أن الاسم الذي يستخدمه الموقع هو اسم مستعار.
- إبلاغ مقدم خدمات ثقة الذي يقوم بإثبات صحة التوقيع الإلكتروني بذلك.

المحور السادس: خدمة الإرسال الإلكتروني المضمون وعلاقته بالتوقيع الالكتروني

تعادل خدمة الإرسال الإلكتروني المضمون الإرسال البريدي المضمون المتعارف عليه، ويهدف إلى إرسال واستلام المعطيات الإلكترونية بشكل آمن وبكل ثقة، كما تضمن هذه الخدمة صحة تاريخ إرسال واستلام هذه المعطيات.

وتعتمد خدمة الإرسال الإلكتروني المضمون على التوقيع الالكتروني، حيث يتم تأمين إرسال واستلام المعطيات الإلكترونية بواسطة التوقيع الإلكتروني أو بواسطة الخاتم الإلكتروني لمقدم خدمات موثوق به.

المحور السابع: العلاقة بين وسائل التشفير وخدمات الثقة

يعتبر التشفير وتحليل الشفرات، وفقا لمشروع هذا القانون، تقنية ترتكز عليها خدمات الثقة المؤطرة بموجبه، حيث تتجلى **وسائل التشفير وتحليل الشفرات** وفقا للمادة 45 في كل معدات أو برمجيات، من أجل تحويل معطيات إلكترونية، أو من أجل إنجاز العملية العكسية. وتهدف وسيلة التشفير وتحليل الشفرات على الخصوص إلى ضمان سلامة تبادل المعطيات بطريقة إلكترونية أو تخزينها، بكيفية تمكن من ضمان سريتها والتيقن منها ومراقبة تماميتها.

ونظرا لعلاقة التشفير وتحليل الشفرات بمجال الدفاع وأمن الدولة، نص مشروع هذا القانون على نظام يخضع استيراد وسائل التشفير وتحليل الشفرات أو تصديرها أو توريدها وكذا تقديم خدمات التشفير وتحليل الشفرات لتصريح مسبق لدى السلطة الوطنية عندما ينحصر الغرض من هذه الخدمة في التيقن من إرسالية أو ضمان تمامية المعطيات المرسلة بطريقة إلكترونية أو لترخيص من قبل السلطة الوطنية عندما يتعلق الأمر بغرض آخر.

كما أن وسائل التشفير تعتبر ضرورية عندما يتعلق الأمر بالتوقيع الالكتروني المؤهل.

المحور الثامن: دور إدارة الدفاع الوطني في تعزيز الثقة الرقمية

لا بد من الإشارة في البداية إلى أن بلادنا قد تبنت "استراتيجية المغرب الرقمي"، حيث تتولى وزارة الصناعة والتجارة والاقتصاد الأخضر والرقمي وضع وتنفيذ استراتيجية التطور الرقمي لبلادنا عبر وكالة التنمية الرقمية التي تضم في مجلس إدارتها ممثلين عن القطاع العام (ممثلين عن القطاعات الحكومية من ضمنها إدارة الدفاع الوطني وبعض المؤسسات العمومية) وممثلي القطاع الخاص، وبالتالي لا يندرج هذا المجال بالأساس ضمن الاختصاصات الموكولة لإدارة الدفاع الوطني التي يتجلى دورها في حماية وتعزيز الأمن والثقة الرقمية.

ولمواكبة هذه الاستراتيجية، انخرطت إدارة الدفاع الوطني منذ سنة 2011، تحت القيادة الرشيدة **لصاحب الجلالة الملك محمد السادس نصره الله وأيده**، في مسار تعزيز القدرات الوطنية لأمن نظم المعلومات وتوطيد الثقة الرقمية، حيث اعتمد المغرب سنة 2012 الاستراتيجية الوطنية للأمن المعلوماتي وكذا التوجيهات الوطنية لأمن نظم المعلومات التي تسري على الإدارات والهيئات العمومية منذ سنة 2014.

ووفقا للمهام المنوطة بقطاع الدفاع الوطني، يتجلى الهدف العام الذي يسعى إلى تحقيقه في تقديم وسائل الحماية الرامية إلى تطوير الثقة الرقمية وتعزيز أمن الاقتصاد الرقمي، تعتمد على مكافحة الهجمات السيبرانية التي تمس بالمعاملات الالكترونية، ولمكافحة هذه الهجمات بشكل أفضل، عملت إدارة الدفاع الوطني على إعداد مجموعة من القوانين التي من شأنها تعزيز استراتيجية الدولة في المجال الرقمي لا سيما القانون المتعلق بالأمن السيبراني.

المحور التاسع: مواكبة تطبيق القانون والحملات التحسيسية

بعد إقرار مشروع هذا القانون وصدوره في الجريدة الرسمية، ستعمل إدارة الدفاع الوطني على تنظيم حملات تحسيسية حول مضامين هذا المشروع حتى يتسنى الاستعمال الأمثل لمختلف خدمات الثقة التي يؤطرها هذا النص، بالإضافة إلى نشر دليل على الموقع الالكتروني للسلطة الوطنية يساعد على حسن استعمال هذه الخدمات وتشجيع مقدمي خدمات الثقة للقيام كذلك بحملات تحسيسية تعرف بهذه الخدمات.

السيد رئيس اللجنة المحترم،
السيدات والسادة المستشارين المحترمين،

تلكم كانت أهم التوضيحات والاجابات بخصوص مداخلاتكم القيمة، ومن أجل إمدادكم بالمزيد من المعطيات التقنية حول مشروع هذا القانون، أضع بين أيديكم ورقة تقنية مبسطة تتضمن مختلف الشروحات والتوضيحات، وختاما أجدد لحضراتكم عبارات تقديري واعتزازي بالتواصل معكم، معبرا لكم عن جزيل الشكر على حسن اهتمامكم.

والسلام عليكم ورحمة الله تعالى وبركاته.

المملكـــــة المغـــربية

إدارة الدفاع الوطني

ملحق:

توضيحات تقنية حول خدمات الثقة بشأن
المعاملات الإلكترونية

أولا: خدمات الثقة

تتمثل خدمات الثقة في ما يلي:

- إنشاء التوقيعات الإلكترونية، أو الأختام الإلكترونية، أو الختم الزمني الإلكتروني، أو خدمات الإرسال الإلكتروني المضمون؛
- إنشاء الشهادات الإلكترونية المتعلقة بالتوقيعات الإلكترونية، أو بالأختام الإلكترونية، أو بالختم الزمني الإلكتروني أو بالتيقن من مواقع الأنترنت؛
- إثبات صحة التوقيعات الإلكترونية أو الأختام الإلكترونية؛
- حفظ التوقيعات الإلكترونية أو الأختام الإلكترونية أو الشهادات المتعلقة بهاتين الخدمتين.

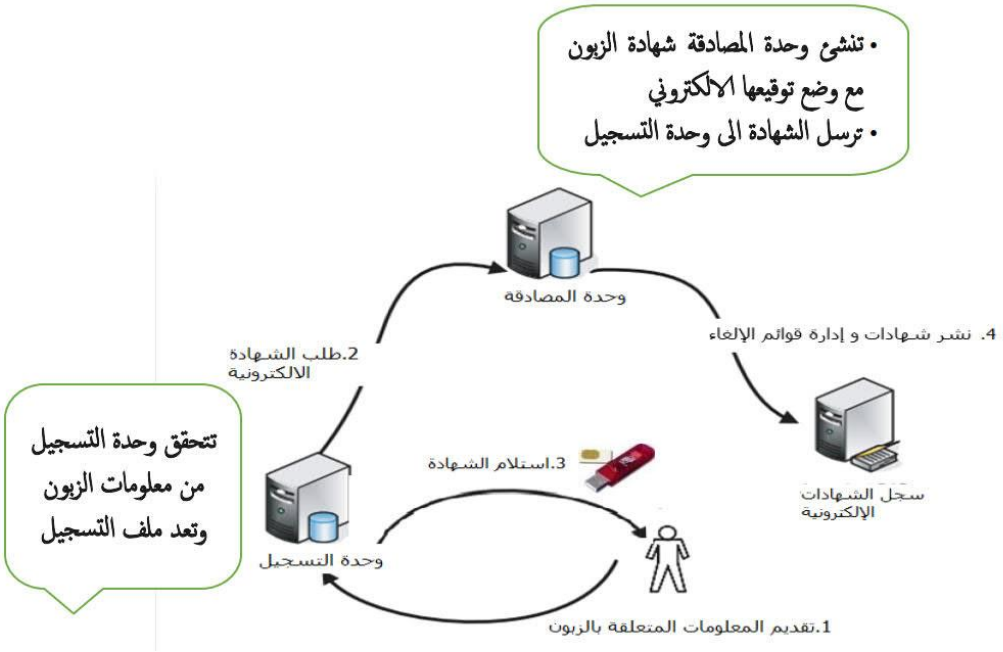
التوقيع الإلكتروني مكون أساسي ترتكز عليه جميع خدمات الثقة الأخرى.

ثانيا: الشهادة الإلكترونية

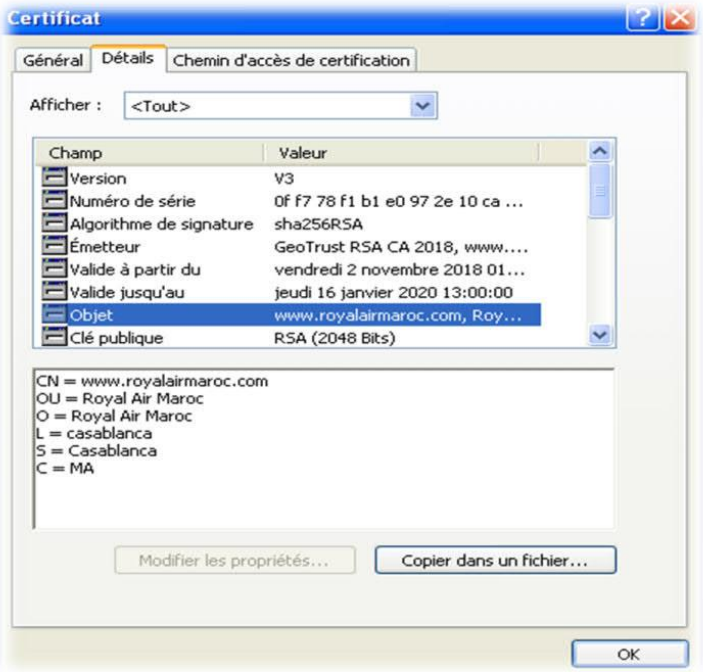
- عبارة عن ملف إلكتروني يحتوي خصوصا على المعلومات الشخصية لصاحب الشهادة، والمعلومات المتعلقة بمقدم خدمات الثقة ومعلومات أخرى، بالإضافة إلى مفتاح الشفرة العمومي الذي يرتبط منطقيًا بمفتاح الشفرة الخاص.
- عند إصدار الشهادة من قبل مقدم خدمات، فإنه يضمن صحة البيانات الواردة فيها ويشهد على ارتباطها بصاحبها.
- يمكن أن تكون الشهادة الإلكترونية إما على شكل برمجية أوعلى شكل آلية (بطاقة ذكية ،أداة مشفرة،...).

1

ثالثا: مراحل استلام الشهادة الإلكترونية



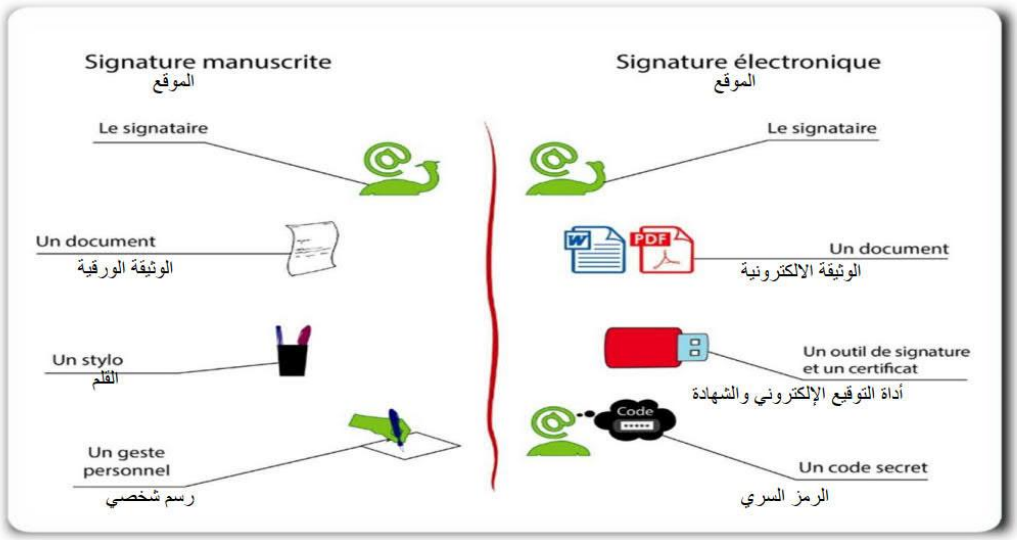
مقتطف مأخوذ من متصفح الأنترنيت لشهادة إلكترونية للخطوط الملكية المغربية



2

رابعا: التوقيع الالكتروني

1. أوجه التشابه والاختلاف بين التوقيع الخطي والتوقيع الإلكتروني وخصائصهما



التوقيع الالكتروني	التوقيع الخطي
يرتكز على عمليات رياضية وتقنية، وبالتالي يصعب تزويره	عبارة عن رسم يقوم به الشخص، مما يجعل تزويره أو تقليده سهلا
يمكن التحقق من صحته بشكل آلي وفوري	يصعب التحقق من صحته
يمكن هذا التوقيع من الحفاظ على تمامية الوثيقة الموقعة	الرسالة الموقعة يمكن المس بتماميتها بسهولة

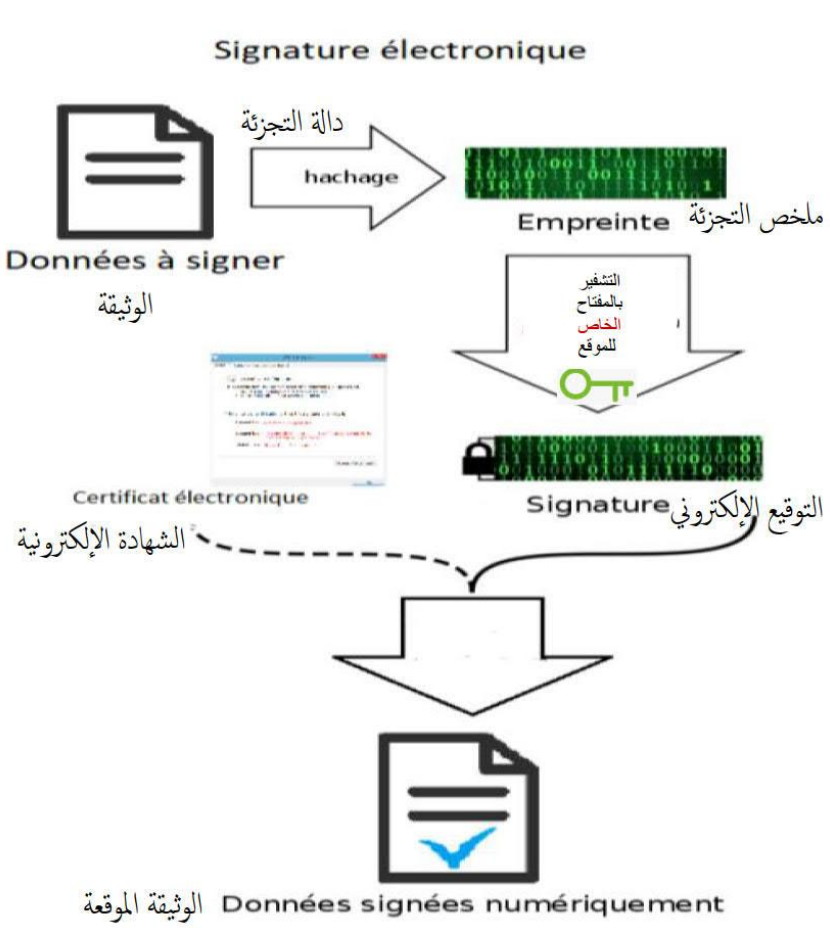
2. ضمانات التوقيع الإلكتروني المرتكز على علم التشفير

هوية الموقّع	• من خلال الشهادة الإلكترونية الصادرة للموقّع
عدم تنصل الموقع من الوثيقة الموقعة	• بفضل المفتاح الخاص الذي يجب أن يكون تحت السيطرة الحصرية للموقع
تمامية الوثيقة الموقعة	• عبر دالة التجزئة وهي عبارة عن عملية رياضية تأخذ نصا مهما كان حجمه وتحوله إلى ملخص بحجم ثابت يميز هذا النص عن غيره

3. عملية التوقيع الإلكتروني

تتمثل عملية إنشاء التوقيع الإلكتروني على النحو التالي:

- يتم تحويل الوثيقة الإلكترونية إلى ملخص تجزئة باستعمال دالة التجزئة ثم ينقل هذا الملخص إلى آلية إنشاء التوقيع الإلكتروني؛
- يتم تشفير ملخص التجزئة بمفتاح الشفرة الخاص للموقّع الموجود على هذه الآلية؛
- ترسل المجموعة المكونة من الوثيقة والتوقيع الإلكتروني للوثيقة والشهادة الالكترونية إلى المستلم، وهذا ما يعتبر وثيقة موقعة.



4. عملية التحقق من صحة التوقيع الإلكتروني

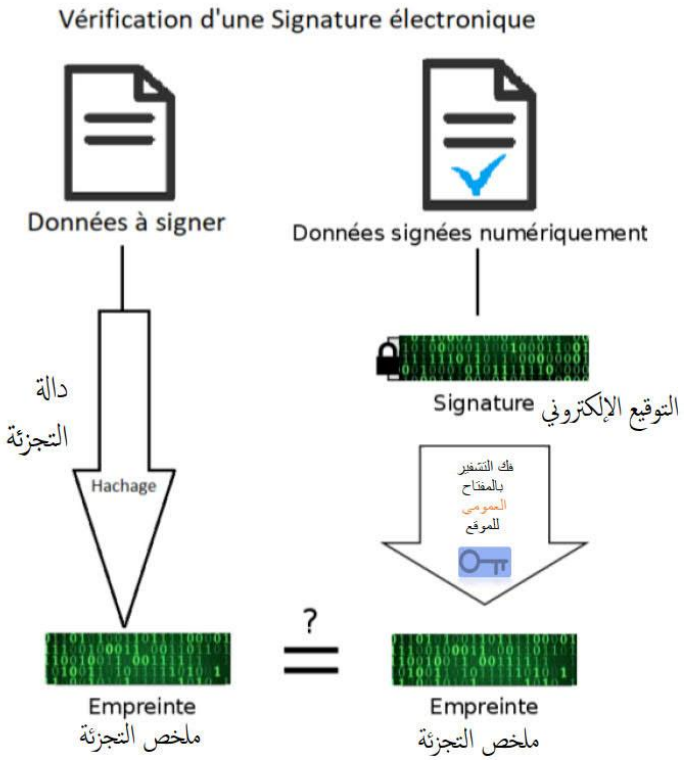
تتم باستخدام مفتاح الشفرة العمومي للموقع الموجود في شهادته الإلكترونية، عن طريق إجراء عملية حسابية عكسية لما سبق.

من أجل ذلك يقارن بين ما يلي :

1. ملخص تجزئة الوثيقة بعد استخدام نفس دالة التجزئة
2. ملخص التجزئة المحصل عليها بعد فك تشفير التوقيع الإلكتروني للوثيقة الموقعة

إذا تطابق ملخصا التجزئة، يعتبر التوقيع صحيحا.

5



Si les empreintes sont identiques, la signature est valide

إذا تطابق ملخصا التجزئة فالتوقيع يعتبر صحيح

6

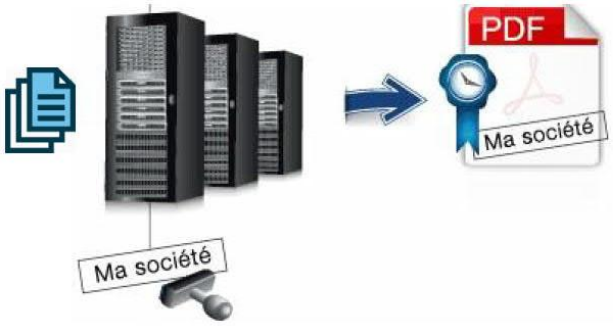
5. مستويات التوقيع الالكتروني

التوقيع الإلكتروني البسيط	• لا يستلزم أي معايير أو متطلبات تنظيمية • الحياد التكنولوجي فيما يخص التقنية المستعملة • لا توجد متطلبات للتحقق من الهوية • مقبول عند التقاضي لكن عبء الاثبات على الموقع • مناسب للمعاملات الإلكترونية البسيطة ذات الرهانات القانونية والمالية المنخفضة.
التوقيع الإلكتروني المتقدم	• يستلزم متطلبات تنظيمية ومعايير محددة • يرتكز على تقنية الشهادة الإلكترونية أو ما يعادلها • يستلزم التحقق من الهوية دون إلزامية الحضور الشخصي • يوجب توفير ملف الأدلة (dossier de preuve)، عند الاقتضاء، من طرف مقدم الخدمات • مناسب للمعاملات الإلكترونية ذات الرهانات القانونية والمالية المتوسطة، خصوصا تلك التي تتطلب توقيع إلكتروني عن بعد
التوقيع الإلكتروني المؤهل	• يستلزم متطلبات تنظيمية ومعايير دقيقة • يفرض استخدام تقنية الشهادة الإلكترونية • يستلزم الحضور الشخصي من أجل التحقق من الهوية • يتمتع بقيمة قانونية عالية: له قرينة الموثوقية كالتوقيع الخطي • موجه للمعاملات الإلكترونية ذات الرهانات القانونية والمالية العالية.

خامسا: الخاتم الإلكتروني

يقدم هذا المشروع الخاتم الإلكتروني كوسيلة لختم الوثائق باسم أشخاص اعتباريين كالشركات والمؤسسات العامة وذلك من أجل ضمان أصل و تمامية هذه الوثائق. **فهو إذن بمثابة نسخة رقمية للطابع الإعتيادي للمؤسسات**.

	التوقيع الإلكتروني	الخاتم الإلكتروني
المستعمل	شخص ذاتي	شخص اعتباري
الإنشاء	عملية يقوم بإجرائها الموقع بشكل مباشر ويتأكد من الوثيقة التي سيوقعها	يمكن القيام به بشكل آلي، يمكن استعماله لختم عدد كبير من الوثائق في آن واحد كالفواتير والشهادات
الأهداف	يعبر عن رضى الموقع و يحافظ على أصل و تمامية الوثيقة	يحافظ على أصل و تمامية الوثيقة



الخاتم الإلكتروني و التوقيع الإلكتروني متشابهان من الناحية التقنية

8

أمثلة لبعض استعمالات الخاتم الالكتروني

سادسا: الختم الزمني الإلكتروني

يتمثل الختم الزمني الإلكتروني في وضع وإدراج تاريخ موثوق به على وثيقة الكترونية ويضمن:

- وجودها في تاريخ معين ؛
- أنه لم يتم تعديلها البتة منذ ذلك التاريخ (مبدأ التمامية).

من الناحية التقنية، تتم عملية الختم الزمني الإلكتروني:

1. عبر إرسال طلب إلى وحدة موثوقة ، تسمى "وحدة الختم الزمني" ،يشتمل الطلب على ملخص تجزئة الوثيقة التي سيتم ختمها زمنيا؛
2. ثم تعيد السلطة إلى صاحب الطلب رمز الختم الزمني ، وملخص التجزئة، والتاريخ والوقت، توقع كل هذه العناصر من طرف سلطة الختم الزمني.

سابعا: إثبات صحة التوقيعات الإلكترونية أو الأختام الإلكترونية

أثناء التوقيع أو وضع الخاتم ، يكون من المعلوم على أن الشهادة الإلكترونية المستعملة صالحة و بالتالي يكون من السهل التحقق من صحة التوقيع أو الخاتم، في حين يكون من الصعب التحقق من ذلك بعد انتهاء مدة صلاحية هذه الشهادة والتي لا تتجاوز عموما ثلاث سنوات.

ومن هنا تأتي أهمية إثبات صحة التوقيع الإلكتروني أو الخاتم الإلكتروني بمجرد وضعها على الوثيقة.

تكون نتيجة هذه العملية عبارة عن تقرير الكتروني مدمج مع الوثيقة الموقعة وفق شكل معياري محدد يحمل توقيع مقدم خدمات الثقة المؤهل.

ثامنا: حفظ التوقيع الإلكتروني أو الخاتم الالكتروني

- تهدف هذه العملية إلى الحفاظ على موثوقية التوقيع الإلكتروني أو الخاتم الإلكتروني إلى ما بعد فترة الصلاحية التكنولوجية للتقنيات المستعملة. مما يمكن من إبقاء القوة الثبوتية للوثيقة الإلكترونية.
- تساعد هذه الخدمة على الحماية من التقادم التكنولوجي أو من خرق الخوارزميات المستخدمة في التوقيعات أو الأختام الإلكترونية.

تاسعا: الإرسال الإلكتروني المضمون

- يعادل الإرسال البريدي المضمون المتعارف عليه، ويهدف إلى إرسال واستلام المعطيات الإلكترونية بشكل آمن وبكل ثقة وكذلك يضمن صحة تاريخ إرسال واستلام هذه المعطيات.
- يتم تأمين إرسال و استلام المعطيات الإلكترونية بواسطة التوقيع الإلكتروني أو بواسطة الخاتم الإلكتروني لمقدم خدمات موثوق به.
- من الناحية التقنية، تتمثل هذه العملية في شكل خدمة إلكترونية، يمكن الولوج إليها عبر منصة على الانترنت يوفرها مقدم خدمات ثقة.

مثال: خدمة إرسال إلكتروني متوفرة على الانترنت

عاشرا: التيقن من مواقع الإنترنت

- تهدف خدمة التيقن من موقع الإنترنت بشكل أساسي ضمان صحة موقع الإنترنت وحقيقة هوية صاحبه (شخص ذاتي أو اعتباري) من خلال شهادة إلكترونية للتيقن من موقع الإنترنت مسلمة من طرف مقدم خدمات الثقة.
- توفر هذه الخدمة لمتصفحي ومستعملي مواقع الإنترنت حماية من هجمات الإنترنت من نوع "التصيد الإلكتروني" أو أي هجمة من هذا القبيل.
- تحتوي الشهادة السالفة الذكر على معلومات عن مقدم خدمات الثقة الذي أصدرها، ومعلومات خاصة بالشخص الذاتي أو الاعتباري الذي يدير موقع الانترنت، بالإضافة إلى اسم المجال الذي يديره هذا الشخص.

11

ملحـــــــــق :
ورقة إثبات الحضور

ROYAUME DU MAROC

PARLEMENT

CHAMBRE DES CONSEILLERS

Commission des Affaires étrangères,
de la défense nationale et des Marocains
Résidant à l'Etranger

PRÉSIDENT

المملكة المغربية

البرلمان

مجلس المستشارين

لجنة الخارجية والدفاع الوطني
والمغاربة المقيمين في الخارج

الرئيس

ورقة اثبات حضور السيدات والسادة المستشارين

تاريخ انعقاد الاجتماع: الثلاثاء 15 دجنبر 2020 على الساعة الحادية عشرة صباحا.

موضوع الاجتماع: الدراسة والتصويت على مشروع قانون رقم 43.20 يتعلق بخدمات الثقة بشأن المعاملات الإلكترونية .

الولاية التشريعية : 2015 -2021

السنة التشريعية : 2020-2021

دورة : أكتوبر 2020

اجتماع رقم : 6

عدد الحاضرين في اللجنة : 9

عدد الحاضرين من أعضاء اللجنة : 9

عدد المعتذرين :

عدد المتغيبين : 10

نسبة الحضور بالنسبة لأعضاء اللجنة :

المدة الزمنية : ساعتان و15 دقيقة

السيدات والسادة المستشارون أعضاء مكتب اللجنة

المهمة	الاسم	الصورة الشخصية	الفريق أو المجموعة البرلمانية	التوقيع
رئيس اللجنة	السيد محمد الرزمة		فريق التجمع الوطني للأحرار	
الخليفة الأول	السيد عمر مورو		فريق الاتحاد العام لمقاولات المغرب	
الخليفة الثاني	السيد سعيد زهير		الفريق الدستوري الديمقراطي الاجتماعي	
الخليفة الثالث	السيد مولاي ابراهيم الشريف		الفريق الاستقلالي للوحدة و التعادلية	المشارك تمت بعد
الخليفة الرابع	السيد الحسين المخلص		فريق الأصالة و المعاصرة	
الخليفة الخامس	السيد نبيل الأندلوسي		فريق العدالة و التنمية	
الخليفة السادس	السيد عبد العزيز بوهدود		فريق التجمع الوطني للأحرار	

البرلمان - مجلس المستشارين - الهاتف : 15/14 83 21 537 (212) - الفاكس : 80 26 73 537 (212)
E-mail : Commissionae@gmail.com

ROYAUME DU MAROC
PARLEMENT
CHAMBRE DES CONSEILLERS
Commission des Affaires étrangères,
de la défense nationale et des Marocains
Résidant à l'Etranger
PRÉSIDENT

المملكة المغربية
البرلمان
مجلس المستشارين
لجنة الخارجية والدفاع الوطني
والمغاربة المقيمين في الخارج
الرئيس

تاريخ انعقاد الاجتماع: الثلاثاء 15 دجنبر 2020 على الساعة الحادية عشرة صباحا.

موضوع الاجتماع: الدراسة والتصويت على مشروع قانون رقم 43.20 يتعلق بخدمات الثقة بشأن المعاملات الإلكترونية.

السيدات والسادة المستشارون أعضاء مكتب اللجنة

الأمين	السيد بنمبارك يحفظه		الفريق الحركي	المشاركة عن بعد
مساعد الأمين	السيدة فاطمة الزهراء اليحياوي		فريق الاتحاد المغربي للشغل	
المقرر	السيد أحمد بولون		الفريق الاشتراكي	
مساعد المقرر	----------		الفريق الاستقلالي للوحدة و التعادلية	

البرلمان - مجلس المستشارين - الهاتف : 15/14 83 21 537 (212) - الفاكس : 80 26 73 537 (212)
E-mail : Commissionae@gmail.com

ROYAUME DU MAROC

PARLEMENT

CHAMBRE DES CONSEILLERS

Commission des Affaires étrangères,
de la défense nationale et des Marocains
Résidant à l'Etranger

PRÉSIDENT

المملكة المغربية

البرلمان

مجلس المستشارين

لجنة الخارجية والدفاع الوطني
والمغاربة المقيمين في الخارج

الرئيس

تاريخ انعقاد الاجتماع: الثلاثاء 15 دجنبر 2020 على الساعة الحادية عشرة صباحا.

موضوع الاجتماع: الدراسة والتصويت على مشروع قانون رقم 43.20 يتعلق بخدمات الثقة بشأن المعاملات الإلكترونية .

السيدات والسادة المستشارون أعضاء اللجنة

الفريق أو المجموعة البرلمانية	الاسم	الصورة الشخصية	التوقيع
فريق الأصالة و المعاصرة	السيد محمد الشيخ بيد الله		المشاركة لن بعد
	السيد الحبيب بن الطالب		
	السيد العربي الهرامي		
	السيدة فاطمة الزهراء بن الطالب		المشاركة لن بعد
الفريق الاستقلالي للوحدة والتعادلية	السيد حمة أهل بابا		المشاركة لن بعد
	السيد أحمد لخريف		

3

البرلمان - مجلس المستشارين - الهاتف : 15/14 83 21 537 (212) - الفاكس : 80 26 73 537 (212)
E-mail : Commissionae@gmail.com

ROYAUME DU MAROC
PARLEMENT
CHAMBRE DES CONSEILLERS
Commission des Affaires étrangères,
de la défense nationale et des Marocains
Résidant à l'Etranger
PRÉSIDENT

المملكة المغربية
البرلمان
مجلس المستشارين
لجنة الخارجية والدفاع الوطني
والمغاربة المقيمين في الخارج
الرئيس

تاريخ انعقاد الاجتماع: الثلاثاء 15 ديسمبر 2020 على الساعة الحادية عشرة صباحا.

موضوع الاجتماع: الدراسة والتصويت على مشروع قانون رقم 43.20 يتعلق بخدمات الثقة بشأن المعاملات الإلكترونية .

السيدات والسادة المستشارون أعضاء اللجنة

فريق العدالة والتنمية	السيد عبد الإله الحلوطي		
الفريق الحركي	السيد سيدي صلوح الجماني		
التقدم والاشتراكية	السيد عبد اللطيف أوعمو		المشاركة عن بعد

البرلمان - مجلس المستشارين - الهاتف : 15/14 83 21 537 (212) - الفاكس : 80 26 73 537 (212)
E-mail : Commissionae@gmail.com