شروط العقد العامة المادة ٢٢	يحق للإدارة، في حال إخلال الملتزم بتنفيذ التزاماته أو التأخر في التسليم أو ظهور تقصير أو عيب في الأعمال، توجيه إشعارات تقصير والتحقيق وإلزامه بالتصحيح على نفقته وضمن المهل المحددة، وإصدار غرامات أو تعويضات مقطوعة وفقاً لشروط العقد.
شروط العقد العامة المادة ٢٣	إصدار غرامات التأخير عن كل أسبوع تأخير: ١- مدة التدريب على التشغيل والتجهيز /$٢٠,٠٠٠/ عشرون ألف دولار أميركي. ٢- التأخير في التسلم والتسليم /$٢٠,٠٠٠/ عشرون ألف دولار أميركي. ٣- لا تنطبق غرامات التأخير في حالات القوة القاهرة المنصوص عنها في القانون اللبناني وكذلك في حالات التأخير التي تكون الإدارة مسؤولة عنها. جدول خاص بالمبالغ المقتطعة: إشعارات التقصير في أسبوع واحد على أن تكون الإشعارات معللة ومرفقة بإثباتات قانونية: ١- من ١ الى ١٠ إشعارات/$١,٥٠٠/ ألف وخمسمائة دولار أميركي عن كل إشعار ٢- من ١١ الى ٢٥ إشعار/$٣,٠٠٠/ ثلاثة الآف دولار أميركي عن كل إشعار. ٣- من ٢٦ إشعار أو أكثر/$٤,٥٠٠/ اربعة الآف وخمسمائة دولار أميركي عن كل إشعار. ٤- إشعار مشدد: يوازي الاشعار المشدد خمس إشعارات بالتقصير. الحد الأعلى لمبلغ التعويضات المقطوعة: ٢٠٪ من قيمة سقف الإيراد السنوي التعاقدي (CARC).
شروط العقد العامة المادة ٢٤ البند٥	تحدد فترة إصلاح أو تبديل اللوازم أو الجزء أو الاجزاء المتضررة خلال فترة ٢٥ يوماً من تاريخ تبلغ الملتزم بالعيب.
شروط العقد العامة المادة ٢٧ البند ٢	نسبة زيادة أو إنقاص كمية أي بند: جدول النشاطات/الاجراءات (البند الثالث-١).
شروط العقد العامة المادة ٣١	تعتبر جميع التجهيزات القائمة والمستحدثة والبرامج الفنية والالكترونية وأسم المستخدم وكلمة المرور (User name & Password) ملكاً للإدارة بعد تسلمها وقبولها.
شروط العقد العامة المادة ٣٢	يباشر الملتزم باتخاذ الاجراءات اللازمة لتسليم كافة انواع التجهيزات والمعدات واللوازم والآليات الى الإدارة و/أو الملتزم الجديد الذي تختاره الإدارة قبل انتهاء العقد بستون يوماً على الاقل وعليه ابلاغ الإدارة بتاريخ المباشرة بهذه الاجراءات.
على الملتزم الفائز بالمناقصة الاستحصال وعلى كامل مسؤوليته على كافة الرخص والمستندات المتوجبة ولا يمكن أن يتذرع بأي سبب للتأخير في أداء مهمته لأي سبب يكون ناتجاً عن عملية الحصول على تلك الرخص.	

الجزء الثالث – العقد

الفصل السابع: ملاحق ونماذج العقد للاشتراك في مناقصة عمومية

موضوع التلزيم: تقديم خدمات تغيير، وصيانة، وتطوير، وتحديث برامج المكننة في مصلحة تسجيل السيارات والآليات، وتأمين بطاقات رخص السوق ورخص السير واللاصقات الالكترونية.

ملحق رقم (١) صيانة التجهيزات الحالية

تتولى الشركة الملتزمة صيانة كافة الأجهزة والبرامج العائدة للإدارة والداخلة ضمن مسؤوليتها التعاقدية، وذلك بصورة شاملة ومتكاملة، بما فيها على سبيل المثال لا الحصر: صيانة أجهزة الخوادم، الحواسيب، أجهزة الشبكات، أنظمة البرمجيات التطبيقية والتشغيلية، وأي تجهيزات تقنية مرتبطة بها.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

ملحق رقم (٢) تعهد/تصريح للاشتراك في مناقصة عمومية

تقديم خدمات صيانة وتطوير وتحديث برامج المكننة في مصلحة تسجيل السيارات والاليات لزوم اصدار رخص سوق ورخص سير المركبات الالية واللاصقات الالكترونية.

أنا الموقع ادناه .....

الممثل بالتوقيع عن مؤسسة/شركة .....

المتخذ لي محل اقامة.....منطقة.....

حي.....شارع.....ملك.....

.....

رقم الهاتف.....، مكتب ..... فاكس .....،

اعترف بانني اطلعت على دفتر الشروط المتضمن التعهد، الشروط الادارية والفنية الخاصة للاشتراك في هذا التلزيم التي تسلمت نسخة عنها.

واصرح انني وبعد الاطلاع على هذه المستندات التي لا يمكن باي حال الادعاء بتجاهلها وعلى تفاصيل الاعمال المطلوبة، وانني اتعهد بقبول كافة الشروط المبينة فيها وبمدة صلاحية العرض المحددة بموجب المادة الثانية عشر من دفتر الشروط هذا وبالتقيد بها وتنفيذها كاملة دون أي نوع من انواع التحفظ او الاستدراك.

وأنني تقدمت لهذا الإلتزام للإشتراك بمناقصة "تقديم خدمات صيانة وتطوير وتحديث برامج المكننة في مصلحة تسجيل السيارات والاليات لزوم اصدار رخص سوق ورخص سير المركبات الالية واللاصقات الالكترونية".

كما اصرح بانني وضعت الاسعار وقبلت الاحكام المدرجة في دفتر الشروط هذا آخذاً بعين الاعتبار كل شروط التلزيم ومصاعب تنفيذه في حال وجوده.

كما أتعهد برفع السرية المصرفية عن الحساب المصرفي الذي يودع فيه أو ينتقل إليه أي مبلغ من المال العام، وذلك لمصلحة الإدارة في كل عقد من أيٍ نوعٍ كان، يتناول مالاً عامًا.

التاريخ _____

ختم وتوقيع العارض

طوابع بقيمة

مليون ليرة لبنانية

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

ملحق رقم (٣) صيغة كتاب ضمان أو كفالة

مصرف] حدد اسم المصرف]

جانب هيئة إدارة السير والآليات والمركبات

الموضوع: كتاب ضمان لصالحكم بناء

لآمر] شركة .....حدد اسم الملتزم بخصوص العقد:

موضوع التلزيم: تقديم خدمات تغيير، وصيانة، وتطوير، وتحديث برامج المكننة في مصلحة تسجيل السيارات والآليات، وتأمين بطاقات رخص السوق ورخص السير واللاصقات الالكترونية.

المرجع: [المرجع المعتمد للعقد] تاريخ: [حدد التاريخ]

إن مصرف اسم المصرف.....حدد عنوان المصرف.....، الممثَّل بالسيد حدد اسم الممثل الرسمي للمصرف.....الموقع عنه أدناه وذلك بصفته حدد المسمى الوظيفي لممثل المصرف الرسمي.....، وبناء للآمر شركة حدد اسم الملتزم.....، يتعهد بصورة شخصية غير قابلة للنقض أو للرجوع عنها بأن يدفع نقداً وفوراً دون أي قيد أو شرط أي مبلغ تطالبونه به حتى حدود [أدخل قيمة الكفالة] ..... $ دولار اميركي، وذلك عند أول طلب منكم بموجب كتاب صادر وموقع منكم دون أي موجب لبيان أسباب هذه المطالبة.

وعليه، يقر مصرفنا صراحة بأن كتاب الضمان هذا قائم بذاته ومستقل كلياً عن أي ارتباط أو عقد بينكم وبين لآمر السيد أو السادة أو الشركة.....[حدد اسم الملتزم].....وبأنه لا يحق لمصرفنا في أي حال من الأحوال ولا في أي وقت كان أن يتذرع بأي سبب مهما كان نوعه أو شأنه أو أن يدلي بأية دفوع من أجل الامتناع أو تأجيل تأدية أي مبلغ قد تطالبوننا به بالاستناد إلى كتاب الضمان هذا. كما يتنازل مصرفنا مسبقاً عن أي حق في المناقشة أو في الاعتراض على طلب الدفع الذي يصدر عنكم أو عن أي مسؤول لديكم، أو حتى أن يقبل أي اعتراض قد يصدر عن السيد أو السادة أو الشركة [حدد اسم الملتزم] .....أو عن غيره أو غيرهم أو غيرها بشأن دفع المبلغ إليكم بناء لطلبكم.

يبقى كتاب الضمان هذا معمولاً به لغاية حدد موعد انتهاء الصلاحية بحسب العقد.....وبنهاية هذه المهلة يتجدد مفعوله تلقائياً إلى أن تعيدوه إلينا أو إلى أن تبلغونا خطياً إعفاءنا منه.

إن كل قيمة تدفع من مصرفنا بالاستناد إلى كتاب الضمان هذا بناء لطلبكم، يخفض المبلغ الأقصى المحدد فيه بذات المقدار.

يخضع كتاب الضمان هذا للقوانين اللبنانية ولصلاحيات المحاكم المختصة في لبنان. وتنفيذاً منا لهذا الموجب، نتخذ لنا محل إقامة في مركز مؤسستنا في [حدد عنوان المصرف المُتّخذ محل اقامة]

المكان والتاريخ: .....

الصفة: .....

الاسم : .....

التوقيع: .....

خاتم المصرف

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - السير العام
وزارة الداخلية والبلديات

ملحق رقم (٤) صيغة كتاب ضمان العرض

مصرف (حدد اسم المصرف)

جانب هيئة ادارة السير والآليات والمركبات

الموضوع: كتاب ضمان لصالحكم بناء لآمر شركة[٣]..... بخصوص مناقصة عمومية:

موضوع التلزيم : تقديم خدمات تغيير، وصيانة، وتطوير، وتحديث برامج المكننة في مصلحة تسجيل السيارات والآليات، وتأمين بطاقات رخص السوق ورخص السير واللاصقات الالكترونية.

المرجع: رقم..... تاريخ.....

إن مصرف..... [اسم المصرف] مركزه [حدد عنوان المصرف]....., الممثَّل بالسيد [حدد اسم الممثل الرسمي للمصرف].....الموقع عنه أدناه وذلك بصفته [حدد المسمى الوظيفي لممثل المصرف الرسمي]، وبناء للآمر شركة [حدد اسم العارض].....، يتعهد بصورة شخصية غير قابلة للنقض أو للرجوع عنها بأن يدفع نقداً وفوراً دون أي قيد أو شرط أي مبلغ تطالبونه به حتى حدود أدخل قيمة الكفالة.....$ دولار اميركي، وذلك عند أول طلب منكم بموجب كتاب صادر وموقع منكم دون أي موجب لبيان أسباب هذه المطالبة.

وعليه، يقر مصرفنا صراحة بأن كتاب الضمان هذا قائم بذاته ومستقل كلياً عن أي ارتباط أو عقد بينكم وبين الآمر شركة ..... [حدد اسم العارض] وبأنه لا يحق لمصرفنا في أي حال من الأحوال ولا في أي وقت كان أن يتذرع بأي سبب مهما كان نوعه أو شأنه أو أن يدلي بأية دفوع من أجل الامتناع أو تأجيل تأدية أي مبلغ قد تطالبوننا به بالاستناد إلى كتاب الضمان هذا. كما يتنازل مصرفنا مسبقاً عن أي حق في المناقشة أو في الاعتراض على طلب الدفع الذي يصدر عنكم أو عن أي مسؤول لديكم، أو حتى أن يقبل أي اعتراض قد يصدر عن شركة[حدد اسم العارض] أو عن غيرها بشأن دفع المبلغ إليكم بناء لطلبكم.

يبقى كتاب الضمان هذا معمولاً به لغاية..... [حدد موعد انتهاء الصلاحية] بحسب دفتر الشروط وبنهاية هذه المهلة يتجدد مفعوله تلقائياً إلى أن تعيدوه إلينا أو إلى أن تبلغونا خطياً إعفاءنا منه.

إن كل قيمة تدفع من مصرفنا بالاستناد إلى كتاب الضمان هذا بناء لطلبكم، يخفض المبلغ الأقصى المحدد فيه بذات المقدار.

يخضع كتاب الضمان هذا للقوانين اللبنانية ولصلاحيات المحاكم المختصة في لبنان. وتنفيذاً منا لهذا الموجب، نتخذ لنا محل إقامة في مركز مؤسستنا في [حدد عنوان المصرف] المُتّخذ محل إقامة.

المكان والتاريخ	المكان والتاريخ
الصفة	الصفة
الاسم	الاسم
التوقيع	التوقيع وختم المصرف

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
المدير العام
وزارة الداخلية والبلديات

ملحق رقم (٥) تصريح النزاهة[٤]

عنوان الصفقة: _____

الجهة المتعاقدة:

_____

اسم العارض / المفوض بالتوقيع عن الشركة:

_____

إسم الشركة: _____

نحن الموقعون أدناه نؤكد ما يلي:

١- ليس لنا، أو لموظفينا، أو شركائنا، أو وكلائنا، أو المساهمين، أو المستشارين، أو أقاربهم، أي علاقات قد تؤدي إلى تضارب في المصالح بموضوع هذه الصفقة.

٢- سنقوم بإبلاغ هيئة الشراء العام والجهة المتعاقدة في حال حصول أو اكتشاف تضارب في المصالح.

٣- لم ولن نقوم، ولا أيّ من موظفينا، أو شركائنا، أو وكلائنا، أو المساهمين، أو المستشارين، أو أقاربهم، بممارسات احتيالية أو فاسدة، أو قسرية أو مُعرقلة في ما يخص عرضنا أو اقتراحنا.

٤- لم نقدم، ولا أيّ من شركائنا، أو وكلائنا، أو المساهمين، أو المستشارين، أو أقاربهم، على دفع أي مبالغ للعاملين، أو الشركاء، أو للموظفين المشاركين بعملية الشراء بالنيابة عن الجهة المتعاقدة، أو لأي كان.

٥- في حال مخالفتنا لهذا التصريح والتعهد، لن نكون مؤهلين للمشاركة في أي صفقة عمومية أياً كان موضوعها ونقبل سلفاً بأي تدبير إقصاء يُؤخذ بحقنا ونتعهد بملء إرادتنا بعدم المنازعة بشأنه.

٦- إن أي معلومات كاذبة تُعرضنا للملاحقة القضائية من قبل المراجع المختصة.

التاريخ: _____

الختم والتوقيع

_____

[٤] يُرفق هذا التصريح بالعرض

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

ملحق رقم (٦) نموذج العقد

رقم: ..... فيما بين:

١- الجمهورية اللبنانية، وزارة الداخلية والبلديات – هيئة إدارة السير والآليات والمركبات ممثلة بشخص:
..... رئيس مجلس إدارة ومدير عام هيئة ادارة السير والآليات والمركبات
(المشار اليه فيما يلي بـ "الإدارة")

٢- أدخل اسم الملتزم.....، ممثلا بشخص..... (والمشار إليه فيما يلي بـ "الملتزم")

بناء على المرسوم رقم ..... تاريخ .../.../.... (الموضوع)؛

بناء على قانون الشراء العام؛

بناءً على دفتر الشروط الخاص رقم.... المرجع المعتمد للصفقة تاريخ دفتر الشروط الخاص بالصفقة؛

وبناء على ملف المناقصة المرفق ربطاً؛

وبناء على محضر لجنة دراسة وتقييم العروض المشكلة بموجب القرار رقم.... تاريخ.../..../..... المرفق صورة عنه.

تم الاتفاق على ما يلي:

المادة الأولى: تعتبر المقدمة جزءاً لا يتجزأ من هذا العقد.

المادة الثانية: يتعهد الملتزم "صيانة وتطوير وتحديث وتغيير برامج المكننة في مصلحة تسجيل السيارات والاليات لحساب الإدارة بحسب ما ورد في دفتر الشروط وفق بيان الأسعار التالي:[أدخل بيان الأسعار]

المادة الثالثة: القيمة المرجعية لمشروع الشراء هي..... بالأرقام..... (والعملة).

بالأحرف.....(والعملة) فقط لا غير وتتضمن هذه القيمة تلزيم جميع اللوازم وتأمين جميع الخدمات ذات الصلة والمطلوبة في دفتر الشروط الخاص. تقوم الإدارة بدفع مستحقات الملتزم طبقاً لشروط العقد.

المادة الرابعة: يتعهد الملتزم تسليم البنود المذكورة في المادة الثانية أعلاه في مدة أقصاها تلك المحددة في شروط العقد الخاصة.

المادة الخامسة: يتعهد الملتزم باحترام جميع شروط التنفيذ ومن ضمنها الخدمات ذات الصلة بحسب شروط العقد المرفقة ربطاً مع هذا الاتفاق، والمتضمنة "تقديم خدمات تغيير، وصيانة، وتطوير، وتحديث برامج المكننة في مصلحة تسجيل السيارات والآليات، وتأمين بطاقات رخص السوق ورخص السير واللاصقات الالكترونية". وذلك لصالح هيئة ادارة السير والآليات والمركبات.

المادة السادسة: يتعهد الملتزم بتطبيق كافة البنود الواردة في العرض الذي تقدم به، والمرفق ربطاً. كما يتعهد بتطبيق جميع شروط العقد العامة والخاصة المرفقة بهذا العقد.

المادة السابعة: على الملتزم أن يقدم كفالة مالية لضمان حسن التنفيذ إلى الفريق الأول بالقيمة والشروط والشكل المحددة في شروط العقد العامة، وبإيداعه كل المستندات الادارية والقانونية المطلوبة ومنها براءة ذمة صادرة عن الصندوق الوطني للضمان الاجتماعي.

المادة الثامنة: نظمت هذه الاتفاقية على نسخة واحدة، أصلية بيد الإدارة وصورة عنها بيد الملتزم.

بيروت في: / / ٢٠

الطرف الثاني: الملتزم
اسم الشركة الملتزمة
اسم الشخص المفوض بالتوقيع عن الشركة

التوقيع والختم

الطرف الأول: الإدارة
هيئة ادارة السير والآليات والمركبات
رئيس مجلس إدارة ومدير عام هيئة ادارة السير والآليات والمركبات

التوقيع والختم

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

ملحق رقم (٧) نموذج رسالة تبليغ بتصديق العقد

اسم وعنوان الملتزم :أدخل الاسم والعنوان]

موضوع التلزيم: تقديم خدمات تغيير، وصيانة، وتطوير، وتحديث برامج المكننة في مصلحة تسجيل السيارات والآليات، وتأمين بطاقات رخص السوق ورخص السير واللاصقات الالكترونية.

المرجع: رقم..... تاريخ .../...../ ٢٠

السادة: ..... [اسم الشركة التي رسا عليها التلزيم]
المحترمين،

يسرّ هيئة ادارة السير والآليات والمركبات أن تبلّغكم تصديق العقد المشار اليه أعلاه,

وعليه، تم توقيع العقد من قبلنا، وبإمكانكم الحصول على نسخة موقعة منه من عنواننا التالي: كورنيش النهر – مبنى هيئة ادارة السير والآليات والمركبات.

وبحسب شروط العقد، يجب تقديم ضمان حسن التنفيذ (أو كفالة حسن التنفيذ) خلال مهلة عشرة أيام من تاريخ استلامكم هذا الكتاب وذلك قيمة ٧٪ من القيمة المرجعية للعقد . وعند تقديم الضمان بالشكل والمضمون المطلوبين، بإمكانكم استرداد ضمان العرض.

كما ويتوجب تسديد رسم الطابع المالي بنسبة أربعة بالألف من قيمة الالتزام السنوية، وذلك خلال خمسة ايام عمل من تاريخ هذا التبليغ. إن التأخر في تسديد رسم الطابع المالي تعرضكم لغرامة مالية تعادل خمسة أضعاف قيمة الرسم المتوجب.

بناءً على ما تقدم، نبلّغكم بأن موعد البدء بتنفيذ العقد هو[حدد التاريخ أو الفترة بحسب شروط العقد].

الاسم / المسمى الوظيفي: رئيس مجلس إدارة ومدير عام هيئة ادارة السير والآليات والمركبات بالتكليف
الإدارة: هيئة ادارة السير والآليات والمركبات
التوقيع:
التاريخ

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

ملحق رقم (٨) متطلبات رخص السير الالكترونية

Vehicle Registration Card — Specs & Design

١) Standards & Legal

- ID-١ format; ٨٥.٦٠ × ٥٣.٩٨ mm, ٠.٧٦ mm thick.
- Substrate: polycarbonate (PC), multi-layer, laser-engravable.
- Conformance: ISO/IEC ٧٨١٠ (ID-١); ISO/IEC ٧٨١٦-١ physical characteristics٢) Required Secure Contactless Chip (In-Card)
- Embedded contactless integrated circuit operating at ١٣.٥٦ MHz.
- Interface compliance: ISO/IEC ١٤٤٤٣ (Type A or B) including ISO/IEC ١٤٤٤٣-٤.
- Command set / data access: ISO/IEC ٧٨١٦-٤ (APDUs) with secure messaging and mutual authentication.
- RF/electrical conformance testing: ISO/IEC ١٠٣٧٣-٦ (or equivalent).
- Anti-skimming / anti-eavesdropping controls; personalization keys and crypto profile per Authority policy.
- (Optional if requested) NFC Forum Type ٤ interoperability.
- Chip file structure, keys/algorithms, and data model will be provided only to the awarded vendor.

٢) Product Overview — Front / Back

- Front: national legends, document title, state emblems, owner/registration fields (registration no., owner name, residence, ownership dates).
- Back: vehicle specifications (make, model/year/type, usage category, color, engine/chassis/VIN, seating/weights, other regulatory entries).
- Bilingual artwork (Arabic + French/English). Clear inspection zones reserved.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

٣) Ultraviolet Invisible Inks — Front / Back

- UV-responsive elements present on both sides for rapid field checks.
- Motifs/text visible only under UV illumination.
- Exact spectra/locations will be provided to the awarded vendor.

٤) Printing Securities Overview — Front

- Complex guilloché backgrounds/rosettes.
- Rainbow (split-fountain) transitions in security bands.
- Microprinting (positive & negative).
- Embedded anti-copy cues (e.g., deliberate character variations).
- Precise strings/positions will be provided to the awarded vendor.

٥) Printing Securities Overview — Back

- Matching guilloché program and rainbow transitions.
- Positive microtext bands and mirrored anti-copy cues.
- Precise strings/positions will be provided to the awarded vendor.

٦) Customer Personalization — Front / Back

- Laser-engraved variable data: owner name (Arabic/Latin), registration/record numbers, dates; full vehicle data on back.
- Optional raised/tactile element for quick inspection.
- Optional machine-readable element (١D/٢D) if required by the Authority.

٧) OVD — Front / Back

- Front: one circular OVD/OVE (≈٢٢ mm class) or equivalent.
- Must provide multi-axis Level-١ visual effects (tilt motion/contrast/color), Level-٢ loupe features, and Level-٣ forensic features.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

- Back: OVD optional (if specified by the Authority).
- Detailed effects, iconography, tolerances will be provided to the awarded vendor.

٨) Rainbow Print — Front / Back

- Security split-fountain color transitions with seamless joins across fine lines to resist digital recomposition.

٩) Pre-Personalization — Front / Back

- Pre-printed legends, guilloché backgrounds, microtext bands.
- Registered clear spaces for OVD and inspection windows.
- Blanks delivered ready for Authority personalization workflow.

١٠) Overview View

- Full front/back layouts indicating high-level placement of legends, security zones, OVD, chip area, and personalization blocks .

١١) Viewing Guide — ١st-Line Features (Unaided Eye)

- Tilt left/right and to-and-fro; rotate in plane to observe defined visual changes (motion, contrast, color; rainbow transitions; OVD effects).
- Tactile element check (if used).

٢nd-Line Features (Loupe)

- Verify microprinting and selected covert design elements with an ٨–١٠× loupe.

١٢) Forensic Features (Laboratory)

- Restricted micro/nano and spectral features for lab verification; methods/thresholds shared post-award.

١٣) Durability, Manufacturing & Acceptance

- Minimum ١٠-year service life; resistance to abrasion, UV, humidity/sweat, solvents (spot test), temperature cycling, flex/bend, and delamination—per relevant ISO/industry methods.
- Pilot First Article prior to mass production; acceptance includes checks of artwork fidelity, personalization quality, and functional verification of UV /OVD and contactless chip features.

Confidentiality Note (Public RFP)

All exact design files, placement maps, ink specifications, OVD effects, microtext strings, chip data model/cryptography, and other sensitive security details are intentionally withheld from this public RFP and will be provided only to the awarded vendor following contract award and required confidentiality undertakings.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

ملحق رقم (٩) متطلبات رخص السوق الالكترونية

Driving License Specs and Design

١) Standards & Legal

• ID-١ format; ٨٥.٦٠ × ٥٣.٩٨ mm, ٠.٧٦ mm thick.

• Substrate: polycarbonate (PC), multi-layer, laser-engravable.

• Conformance to ISO/IEC ٧٨١٠ (ID-١) and ISO/IEC ٧٨١٦-١ physical characteristics, and to ISO/IEC ١٨٠١٣-١, ISO/IEC ١٨٠١٣-٢, and ISO/IEC ١٨٠١٣-٣ (driving-licence physical/data/security).

• Harmonized with principles of the Vienna Convention on Road Traffic (١٩٦٨) and Directive ٢٠٠٦/١٢٦/EC as applicable to document content/readability.

٢) Product Overview

Front (recto)

• National legends and document title,cedar/flag, security features.

• Holder identification data: licence number, name, date of birth, photo; issue/expiry info

Back (verso)

• Category table listing vehicle classes with columns for valid-from / valid-to and codes/restrictions (no vehicle specs).

Language & layout

• Bilingual artwork (Arabic + French/English), with clear areas that can be reserved for inspection/verification zones as needed for your design

٣) Substrate & Layer Build

• PC core with integrated security layers designed for long service life and tamper resistance.

• Registered spaces for optical/security elements and inspection windows.

٤) Printing & Artwork (High Level)

• Complex fine-line guilloché backgrounds both sides.

• Rainbow/split-fountain color transitions (no flat digital gradients).

• Microprinting and anti-copy cues embedded in background design.

• National emblems integrated as secure line-art.

Exact artwork, strings, placements, and line structures will be provided to the awarded vendor.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

٥) Covert/Latent Inks

• Ultraviolet-responsive features present on both sides for field inspection.

• Infrared-responsive/absorbent features for device-assisted checks.

• Vendor to support verification with commonly available inspection tools.

Specific ink spectra and locations will be provided to the awarded vendor.

٦) Optically Variable Security (OVE/OVD & OVI)

• One circular OVE/OVD on the front (≈٢٢ mm class) or functionally equivalent solution.

• Must deliver:

– Level-١ (unaided eye) tilt-based motion/contrast/color effects in more than one axis.

– Level-٢ (loupe) micro-elements.

– Level-٣ (forensic) micro/nano elements for laboratory verification.

• Optically Variable Ink (OVI) color-shift areas on the card (front and/or back) for quick visual authentication

Detailed OVD effects, tolerances, and exact OVI locations/colors will be provided to the awarded vendor.

٧) Secure Contactless Chip (RF, in-card)

• Embedded contactless IC operating at ١٣.٥٦ MHz, compliant with ISO/IEC ١٤٤٤٣ (Type A or B) with ISO/IEC ١٤٤٤٣-٤ protocol.

• Command set and data access aligned with ISO/IEC ٧٨١٦-٤ (APDUs); vendor to support secure messaging and mutual authentication.

• Cryptography/profile (e.g., RSA/ECC, keys, certificates), application file structure, and data elements: to be provided to the awarded vendor.

• Read-range, anti-skimming/anti-eavesdropping controls, and personalization keys to meet Authority policy.

• Electrical/mechanical and RF conformance testing per ISO/IEC ١٠٣٧٣-٦ (or equivalent).

• Optional NFC Forum Type ٤ interoperability if requested by the Authority.

٨) Personalization (Front / Back)

• Laser engraving of all variable data (names in Arabic/Latin, license number, dates; vehicle data on back).

• Ghost image: laser-engraved secondary portrait/miniature (where a portrait is part of the data model) for enhanced authentication.

• Optional raised/tactile component for rapid inspection.

• Optional machine-readable element (١D/٢D) if requested by the Authority.

٩) Pre-Personalization

• Pre-printed static legends, backgrounds, and emblems; registered clear spaces for OVE/OVI and inspection zones.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

١٠) Viewing & Verification (Public)

- **Level-١:** verify by tilting left/right and to-and-fro; rotate in plane—observe defined visual changes (including OVI color-shift).
- **Level-٢:** verify selected features with an ٨-١٠× loupe.
- **Level-٣:** verify restricted features with laboratory equipment per Authority protocol.

١١) Durability & Environmental

- Minimum ١٠-year service life (subject to policy exceptions).
- Resistance to abrasion, UV exposure, humidity/sweat, solvents (spot test), temperature cycling, flex/bend, and delamination—per relevant ISO/industry test methods.

Confidentiality Notice

All exact design files, placement maps, ink specifications, OVD effects, OVI locations, ghost-image layout, chip data model, cryptography, and other sensitive security details are intentionally withheld from this public RFP. These materials will be provided only to the awarded vendor after contract award and execution of the required confidentiality undertakings.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

ملحق رقم (١٠) متطلبات اللاصقات الالكترونية

١) Form Factor & Materials

- Size: ١٠٣ × ٧٠ mm nominal (±٠.٥ mm).
- Substrate: PET ٥٠ µm with layered security print.
- Antenna metallization: Aluminum or copper integrated inlay (vendor to propose).
- Adhesive: Permanent, pressure-sensitive, tamper-evident/destructible (break/VOID on removal).
- Lamination: Clear protective laminate with UV inhibitors; high optical clarity, low haze.
- Application: Inside-glass (adhesive to glass); readable from outside.

٢) Artwork & Visible Security (Public)

- Complex guilloché graphics and national motifs.
- Rainbow (split-fountain) transitions and microprint backgrounds.
- Holographic Authority logo on face, registered to artwork.
- Prominent human-readable ID zone (e.g., YEAR + Plate Number + Serial/Code).
- UV-visible verso mark(s).
- Optional iridescent/micro-embossed accent for rapid field check.
- (Exact strings, linework, placements, and any covert features: withheld; see Confidentiality.)

٣) RFID Technology — UHF

- Standard: ISO/IEC ١٨٠٠٠-٦٣ / EPCglobal Gen٢v٢.
- Region: ETSI ٨٦٥–٨٦٨ MHz (or as authorized by the regulator).
- Memory minimums: EPC ≥ ٩٦ bits; User ≥ ١٢٨ bits; TID locked.
- Read range: ≥ ٦ m through a standard windshield using a ٢ W ERP fixed reader and recommended mounting.
- Security & privacy: Access/Kill passwords; Gen٢v٢ privacy features (e.g., authenticated/untraceable commands).
- Tuning: Optimized for glass mounting; maintain performance across OEM glass and light tint.

٤) Data Model (Public Portion)

- Minimum: Unique serial number mirrored in face print, barcode, and RFID memory.
- Optional (if required): Plate number, issue/expiry dates, issuer codes, checksum/digital signature.
- PII: No personal data printed or encoded.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

٥) Human- & Machine-Readable Markings (١D)

- Symbology: Code ١٢٨ (ISO/IEC ١٥٤١٧).
- Data content: Serial only; same serial in human-readable text and barcode.
- Quiet zones: ≥ ١٠× the X-dimension left/right (min ٢.٥ mm each side).
- X-dimension: ٠.٣٣–٠.٥٠ mm (±٠.٠٣ mm).
- Bar height: ≥ ١٠ mm.
- Print contrast: PRD ≥ ٦٠٪ on applied substrate; matte/low-gloss overlam to minimize glare.
- Orientation: Barcode horizontal; positioned to avoid wiper paths and heater lines.
- Digital signature/checksum (optional): Format/keying shared post-award.

٦) Tamper Evidence

- Irreversible delamination/break or clear VOID reveal on removal; re-use not possible.
- Attempted transfer shall disable RF (e.g., antenna fracture).
- Tamper features remain effective on heated and cold glass.

٧) Environmental & Durability

- Service life on vehicle: ≥ ٣ years.
- Temperature: Storage –٢٠ to +٦٠ °C; operation –١٠ to +٥٠ °C.
- UV exposure: ≥ ١,٠٠٠ h equivalent sunlight (no significant fading; maintain readability).
- Humidity: Withstand ٩٥٪ RH cycling without adhesive failure.
- Chemical resistance: Resistant to common cleaners, wiper fluids, condensation; no residue migration.
- Wash/weather: Resistant to automated car washes and road splash; laminate edges remain sealed.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

٨) Printing & Serialization

- Serialization: Secure, non-repeating variable serialization; vendor to supply ranges and reconciliation files.
- Color management: Preserve split-fountain joins and microprint legibility.

٩) Packaging & Delivery

- Format: Rolls or sheets; dust/UV-protected, humidity-controlled packaging.
- Outer labels: Start/end serials and EPC/TID ranges.
- Data file: Digital serialization table (CSV/JSON).
- Instructions: Mounting/installation guide (Arabic/French/English).

١٠) Installation & Guidance

- Mounting locations: As defined by the Authority; vendor to provide placement guide to optimize RF and avoid wiper paths.
- Application: On dry, clean glass; provide squeegee/tabs for bubble-free install.
- Removal: Must not damage glass; residue removable with standard cleaner.

Confidentiality

All antenna layouts, tuning parameters, covert print maps, serial format rules, EPC/User memory maps, and cryptographic details are intentionally withheld from this public specification and will be provided only to the awarded vendor after contract award and execution of required confidentiality undertakings.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

مرفق رقم ١

Table of Contents

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

١٢. MANDATORY DELIVERABLES

١٣. INTELLECTUAL PROPERTY & LICENSING

١٤. GOVERNANCE & COMPLIANCE

١٥. LEGAL AND REGULATORY COMPLIANCE

١٦. TECHNICAL & SECURITY REQUIREMENTS

١٧. PERFORMANCE REQUIREMENTS

١٨. DATA CENTER AND INFRASTRUCTURE REQUIREMENTS

١٩. TESTING & QUALITY ASSURANCE

٢٠. SERVICE LEVELS, WARRANTY, AND ACCEPTANCE

٢١. RISK MANAGEMENT

٢٢. IMPLEMENTATION TIMELINE

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

Acronyms

Governmental & Institutional Acronyms

Acronym	Full Form
MOIM	Ministry of Interior and Municipalities
DGGS	Directorate General of General Security
MOF	Ministry of Finance
NSSF	National Social Security Fund
AFIS	Automated Fingerprint Identification System
DMS	Document Management System
UTF	Unified Traffic File
UTN	Unified Traffic Number
DGCA	Directorate General of Customs Administration

System & Technical Acronyms

Acronym	Full Form
API	Application Programming Interface
CMS	Content Management System
ERP	Enterprise Resource Planning
ETL/ELT	Extract, Transform, Load / Extract, Load, Transform
DBMS	Database Management System
SQL	Structured Query Language
REST	Representational State Transfer
JSON	JavaScript Object Notation
mTLS	Mutual Transport Layer Security
ULID/UUIDvV	Universally Unique Lexicographically Sortable Identifier
WORM	Write Once Read Many
RFID	Radio-Frequency Identification
QR	Quick Response (Code)
VIN	Vehicle Identification Number
NOC / e-NOC	No-Objection Certificate / Electronic NOC
KPI	Key Performance Indicator
BPMN	Business Process Model and Notation
DMN	Decision Model and Notation

Security & Compliance Acronyms

Acronym	Full Form
PCI-DSS	Payment Card Industry – Data Security Standard
ISO/IEC ٢٧٠٠١	Information Security Management System
KYC / AML / CFT	Know Your Customer / Anti-Money Laundering / Counter Financing of Terrorism
PKI	Public Key Infrastructure
HSM	Hardware Security Module
OTP	One-Time Password
SLA	Service Level Agreement
UAT	User Acceptance Testing
DR / DRP	Disaster Recovery / Disaster Recovery Plan
SI	Systems Integrator
MDM	Master Data Management
DQ	Data Quality
APM	Application Performance Monitoring
WCAG	Web Content Accessibility Guidelines

Functional & Operational Acronyms

Acronym	Full Form
PoA	Power of Attorney
IDP	International Driving Permit
ANPR	Automatic Number Plate Recognition
IVR	Interactive Voice Response
SI	Systems Integrator
QA / QC	Quality Assurance / Quality Control
MoF Sanadiq al-Maliyyeh	Ministry of Finance Cashier Counters
e-Gov	Electronic Government

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

Technical Requirements for the Integrated Vehicle Registration & Driver Licensing System

١. INTRODUCTION & PURPOSE

This document defines the **Technical Requirements for the Integrated Vehicle Registration and Driver Licensing System** to be implemented under the authority of the national traffic administration. It consolidates the functional, technical, and security specifications necessary to modernize and unify vehicle and driver data management in compliance with national laws and international best practices.

The purpose of this document is to:

- Establish a comprehensive set of technical specifications that govern the design, development, deployment, and operation of the new system.
- Ensure that the solution provides a single source of truth for vehicle and driver information through the Unified Traffic Number (UTN) and Unified Traffic File (UTF).
- Define mandatory functional modules covering vehicle registration, driver licensing, violations and fines, inspections, insurance integration, notary/legal workflows, customs, and stakeholder portals.
- Specify the technical standards and service levels required for interoperability, performance, resilience, accessibility, and user experience.
- Mandate privacy, security, and compliance controls in line with Lebanese Law No. ٨١/٢٠١٨, the Traffic Law, and international frameworks such as ISO ٢٧٠٠١, PCI-DSS, and WCAG ٢.٢ AA.
- Provide the basis for acceptance testing and quality assurance, ensuring the delivered system is secure, reliable, and fit for long-term operation.

٢. SYSTEM OVERVIEW

The following sections define the technical and functional requirements for a comprehensive Vehicle Registration and Driver Licensing System for the Traffic and Vehicle Management Authority (referred to as Authority). The platform shall digitize and orchestrate all current and future Authority services and authorizations across its mandate, on a modular, secure, and scalable architecture that is configurable rather than hard-coded. The selected integrator (referred to as SI) will provide,

implement, and maintain all solution components in line with modern engineering and best security practices, while reusing or integrating existing Authority assets–upon written approval from the Authority– where this adds value and meets the stated requirements.

Authority Handover Package (Existing System). The Authority will provide the SI with available artifacts from the current system. These materials are reference only, not authoritative requirements; the SI shall validate and normalize them during discovery.

٣. CROSS–CUTTING STANDARDS

١.١. Unified Traffic Number (UTN) – Immutable Master Key.

The Platform shall have the following properties:

- Issue a UTN as a non–guessable, immutable, globally unique identifier that acts as the foreign–key of record across all modules and partner APIs.
- The UTN carries no personal data (non–PII) and is safe to expose in QR/URLs.
- UTN namespaces shall distinguish entity types (e.g. P– Person/UTF, L– Legal Entity, V– Vehicle, C– Case/Service).
- Format: ULID/UUIDv٧ or equivalent with a check digit (e.g. ISO/IEC ٧٠٦٤ mod–٩٧).
- Collisions must be cryptographically improbable.
- UTNs are never re–issued; deactivated records retain their UTN with a terminal status.

١.٢. Digital Archiving & DMS Integration:

The Contractor shall integrate the solution with the Authority's existing Document Management System (DMS) and perform any necessary adjustments/configuration to support all modules that digitize or use documents.

At minimum, the integration will: (i) send documents and metadata from business workflows to the DMS; (ii) enable two–way linkage between records and their documents; and (iii) surface DMS search/preview/audit features.

The Contractor shall integrate with the Authority's DMS to archive documents and metadata from all enabled modules. Where the e–sticker feature is activated per §١.٢٨.٢, the DMS shall retain sticker–lifecycle artifacts (e.g., encoding logs, spoilage images, issuance forms, transfer/replacement approvals) under immutable WORM policies, with bidirectional links to the associated Vehicle ID and (when applicable) RFID EPC.

١.٣. Core Database and Integration Hub:

١.٣.١. At the heart of the system, a central database (preferred relational SQL database for reliability and ACID compliance) will store all data. A services integration hub or API layer

must expose and manage communications between modules and with external systems. This ensures that each component can interoperate seamlessly. The architecture shall be service-oriented or microservices-based, allowing different services (registration, licensing, payments, etc.) to function independently but cohesively. The integration layer will handle things like: calls to the AFIS (fingerprint system) for identity verification, communication with the payment gateway, pushing updates to an external government portal (if needed), or receiving data from insurance and inspection systems and external government systems. All external integrations shall use secure web services or APIs with authentication and encryption.

Plate Contractor Scope Clarification — Hardware Only (No Software Development)

For the avoidance of doubt: the Plate Contractor's scope under this procurement is limited to the supply, production, QA, and handover of secure license plates and related consumables, and the operation of Authority-provided tools. The Plate Contractor is not required to design, host, or develop any software, APIs, integrations, or data interfaces. All digital interfaces, orchestration, portals, and adapters required to interact with plate production are designed, built, hosted, and supported by the Systems Integrator (SI). The Plate Contractor may perform status updates and accept work orders via the Authority-hosted Contractor Portal and/or SI-provided edge software/agents. Any programmatic integration by the Plate Contractor is strictly optional and at the Authority's discretion.

١.٤. API Design & Lifecycle

All synchronous integrations shall use REST/JSON with Open API ٣.x specifications; event streams and webhooks shall use Async API ٢.x. Provide a public sandbox, mock servers, example payloads, and a conformance test suite. Enforce idempotency keys for POST/PUT, cursor-based pagination, structured error taxonomy, per-client rate limits, and mTLS. Backward-compatible changes follow a documented policy; breaking changes require a new major version (URI or Accept header) and ≥ ١٨٠ days deprecation notice.

The SI shall deliver: (a) internal Sticker Supply/Encoding APIs (covering in-scope media/devices); and (b) an Authority-hosted Contractor Portal and file-based job packages for plate production (no API development is required from the Plate Contractor). Where on-prem edge software/agents or device drivers are needed to drive embossing/printing equipment, the SI shall supply, install, and support them.

Non-exhaustive list:

- Entities: Plate Series, Plate Blank (id, batch/lot, material, format), Plate Order, Plate Produced, Plate Issued, Plate Returned, Plate Destroyed, Sticker Roll (UID range), StickerTag (EPC/UID), Sticker Order, Sticker Encoded, Sticker Issued, Sticker Replaced, QA Result.
- Events (webhooks): plate order created, plate order accepted, plate produced, plate qc failed, plate shipped, plate received, sticker roll received, sticker encoded, sticker issued, sticker spoiled, sticker deactivated.

  Note: Events are emitted by the Authority platform. The Plate Contractor is not required to host webhooks; notifications may be consumed via the Contractor Portal and email/SMS. the SI provides the necessary adapters without imposing development obligations on the Plate Contractor.

  Contractor interactions. An Authority-hosted Plate Contractor Portal Developed by the SI is mandatory and sufficient for all plate-related interactions (work-order receipt, QA/acceptance, shipment, receipt, returns). No software development or API hosting is required from the Plate Contractor.

  E-sticker operations are fully provided and operated by the SI under this RFP. Any sticker-related programmatic APIs and sandbox are internal/SI-hosted for Authority use and onboarding of Authority-approved integrators; there is no external sticker contractor. The platform emits event/notification updates; the Plate Contractor may rely on the Portal and notifications alone.
- Compliance: Per-item and per-batch audit trail with signatures, operator IDs, and device IDs.

١.٥. Data Migration Utilities:

Since the new system will replace an existing system, tools or scripts are required to migrate legacy data (vehicle records, driver records, history of transactions, etc.) into the new database. The system shall account for cleaning up or flagging inconsistent data. For example, if the same person has multiple records in legacy data, a merge procedure may be needed to create one unified profile. The vendor shall plan and execute a full data migration as part of the implementation, ensuring minimal disruption. This includes importing archival documents if they have been digitized by an external project and if not to be digitized by the contractor.

Definition — Migration (Canonical).

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

"Migration" means the one-time, end-to-end, auditable transfer and reconciliation of all authoritative data and artifacts from legacy systems into the new Platform, executed on-premises under Authority custody. Scope includes (non-exhaustive): Persons/UTF (with UTN backfill and alias maps), Vehicles, Licenses, Violations & Points, Payments & Receipts, Appointments, Inspection results, Insurance links, Notary/PoA events, Liens/Holds/Impounds, Enforcement artifacts, User accounts/roles, Configuration/reference tables, and all in-scope documents/media in the DMS.

Constraints: No data export off-site; masking/anonymization in lower environments; chain-of-custody and hash manifests for all loads; repeatable runs.

Quality & Acceptance: Authority-approved mappings; ≥٩٩.٩٥٪ record-level integrity on required fields; zero Critical referential-integrity errors; ≤٠.١٠٪ unresolved duplicate candidates post-dedupe; full reconciliation reports (source→target counts, sums, hashes). At least two rehearsal runs in PRE-PROD with signed go/no-go criteria; cutover/rollback plans tested.

١.٦. **Disaster Recovery and Backup Procedures:**

Automation of regular backups and providing the ability to fail over to a disaster recovery environment. The operations of backup/restore shall be as automated as possible, with minimal manual steps to recover functionality in case of failure.

٤. GENERAL SYSTEM REQUIREMENTS AND ARCHITECTURE

This section defines the overarching technical standards, design principles, and quality attributes that the new system must adhere to. The goal is to ensure the delivered solution is modern, scalable, secure, and maintainable over the long term, in line with international best practices and the Lebanese e-government strategy.

١.١. Technology Stack and Architecture: The system shall be built using modern, widely supported technologies. utilizing microservices architecture. The database shall be a robust SQL-based relational database management for reliable transaction handling. The use of microservices (or at least a modular, service-oriented architecture) will ensure that different functional modules can be developed, deployed, and scaled independently as needed. Bidders can propose alternate stacks if they offer compelling advantages, but compatibility, support, and scalability must be demonstrated. The system shall follow a multi-tier architecture separating the user interface, application logic, and data layers, to allow for flexibility in updates and maintenance.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

١.٢. Content Management & ERP Hooks: The solution shall include a built-in Content Management System (CMS) to create, approve, and publish public content (pages, advisories, FAQs, forms, service guides) from a single console with versioning and audit. In addition, provide Enterprise Resource Planning (ERP) hooks (or embedded modules) to streamline internal operations: collections reconciliation, consumables procurement (cards/stickers/plates), and HR-driven role provisioning. Clearly state which ERP capabilities are in-scope vs. to be integrated externally.

١.٣. Standards Compliance and Interoperability: All software components must adhere to open standards to facilitate interoperability. For example, data exchange formats shall use JSON over RESTful APIs for integration with external parties. Where applicable, international standards shall be followed:

١.٣.١. Applicable Technical Standards

- For driving license and vehicle registration cards (smart cards) follow relevant ISO standards.
- For biometric data (fingerprints), ensure templates are compatible with ANSI/NIST or ISO standards so they can integrate with the existing AFIS.
- For data encoding (barcodes, QR codes, RFID), use standard formats so that law enforcement or other systems can read them.

  The system must be built in a way to easily integrate with other government systems in the future (for instance, a national single sign-on, or data exchanges with the Customs Authority, etc.). An API layer or middleware shall make integrations manageable and secure. All internal and partner APIs shall accept UTN as a primary selector and emit UTN in responses and audit logs. Verification endpoints must accept plate, VIN, QR token, or UTN and resolve to the same record. QR payloads shall embed UTN plus a detached signature—no PII.

١.٤. Localization and Language Support: The application (user interfaces for both staff and public portals) shall support multiple languages, primarily Arabic, English and French. All static text, field labels, and messages shall be externalized for easy translation. The system must properly handle Arabic content (RTL display, correct encoding for Arabic names and data) as well as English/French data, reflecting the multilingual nature of Lebanese administration. Reports and printed documents might need to be generated in Arabic (official format) and possibly bilingual; the system shall accommodate such templates.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

Search normalization for Arabic names requirements include: diacritics-insensitive, Alef/Ya/Hamza variants handling, optional transliteration fields, and configurable approximate matching to reduce false negatives.

١.٥. Observability: Provide centralized logging, metrics, traces (APM), alerting, defined log retention timelines, and synthetic monitoring for portals/APIs. Dashboards must be available to Authority ops.

١.٦. Change, Release & Environment Management:

١.٦.١. Environments: DEV, TEST, UAT/PRE-PROD, SEC (Security Testing), and PROD with strict segregation. SEC is a production-parity environment dedicated to third-party security testing.

١.٦.٢. Release train: regular cadence (e.g. every ٢–٤ weeks) with semantic versioning and release notes.

١.٦.٣. Deployment: blue/green or canary with automated health checks and one-click rollback.

١.٧. User Experience and Accessibility:

Emphasis shall be placed on an intuitive, user-friendly interface for both the public-facing portal/mobile app and the internal staff system. Screens shall be logically organized by workflow, minimizing training needs for staff and simplifying the steps for citizens. The portal shall employ responsive web design to work on various devices and meet basic accessibility standards to ensure inclusivity. The design shall also align with any government UX guidelines if available (for example, a unified government e-service style). Wizards and guided processes shall be used for complex tasks so users clearly understand requirements at each step (as noted for the renewal process).

١.٨. Accessibility & UX Performance Targets:

١.٨.١. All web and mobile touchpoints shall conform to WCAG ٢.٢ AA, verified by an independent audit prior to go-live. UX KPIs: (i) Time to Interactive (TTI) P٩٥ $\leq$ ٢.٠s on reference devices; (ii) Search responses $\leq$ ١.٥s P٩٥; (iii) Upload success rate $\geq$ ٩٩.٧٪ monthly; (iv) Client-visible error rate $\leq$ ٠.٥٪ of requests. Accessibility and performance regressions are release-gated and reported in release notes.

١.٩. Performance and Scalability: The system must be capable of handling current transaction volumes and projected growth over at least the next ١٠ years. This includes:

١.٩.١. Performance & Resilience Testing: Load and stress tests shall use production-like mixes (read/write ratios, peak burstiness, feature flags enabled), realistic think times, and anonymized/masked datasets. Tests must cover failover under load, dependency throttling,

and rollback during canary/blue-green deployments. Results (including resource headroom ≥ ٣٠٪ at peak) are acceptance-gated with artifacts shared to the Authority.

١.٩.٢. Supporting concurrent users (for example, hundreds of staff users across branches and thousands of citizens on the portal simultaneously).

١.٩.٣. Quick response times: key transactions (querying a driver or vehicle record, posting a payment, etc.) shall complete within seconds. The architecture shall minimize latency even when integrating with external services (using techniques like caching frequently used data or asynchronous processing when appropriate).

١.٩.٤. The solution shall be scalable horizontally or vertically. It shall support clustering or load balancing across multiple servers for both application and database to ensure that adding users or new centers will not degrade performance.

١.٩.٥. The design shall avoid single points of failure. Redundancy in components (application servers, database replicas) is expected so that the failure of one node does not bring down the entire service.

١.١٠. High Availability and Reliability:

١.١٠.١. Given the mission-critical nature of vehicle registration and licensing (impacting daily citizen transactions and law enforcement), the system shall achieve high uptime target ٩٩.٩٪. This will be supported by:

١.١٠.٢. Redundant system components and a failover setup.

١.١٠.٣. Robust error-handling in the software to prevent crashes and gracefully handle exceptions (with meaningful messages to users and automatic alerts to support staff).

١.١٠.٤. A queuing mechanism for any asynchronous tasks, so that if any external integration (like bank or insurance service) is temporarily down, transactions are queued and retried rather than lost.

١.١٠.٥. The vendor is expected to provide a maintenance schedule plan that includes minimal downtime deployments (e.g. using rolling updates or after-hours scheduling) and quick rollback procedures in case of issues with new releases.

١.١١. Security and Access Control:

The principle of least privilege shall guide user roles. There shall be multiple user levels (e.g. data entry, supervisor, administrator, auditor, etc.), each with access only to the functions they need. The system shall support strong authentication mechanisms for users (password policies, and support for multi-factor authentication especially for administrative or remote access). Public portal users will authenticate via a secure mechanism as well (potentially integrating with

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

a national digital ID or mobile ID system if available). All data in transit and sensitive data at rest must be encrypted.

١.١٢. Integration with National Systems and Future Expansion:

The system shall not be built in isolation. It needs to integrate with:

١.١٢.١. National Identification Systems: If Lebanon has or introduces a digital ID card or a national citizen registry, the system shall be able to use that for validating individuals (e.g. pulling name and DOB from national ID by entering the ID number or reading an e-ID card). In the future, if digital identities (mobile ID apps or others) are in use, the system could accept those credentials for login or signature.

١.١٢.٢. Automated Fingerprint Identification System (AFIS): Integration with current AFIS is required and the system shall be able to have future full integration with the existing or future AFIS used by the Internal Security Forces or Ministry of Interior for biometric identification or General security directorate. For instance, when issuing a new driving license, the applicant's fingerprint might be captured and sent to AFIS to verify the person's identity (and possibly ensure one person has only one license, or check for any fraud or duplicate). The system shall store the AFIS reference or key to link the biometric record. If AFIS returns data (like confirming identity or indicating the person is flagged), the system shall handle that logic accordingly.

١.١٢.٣. Other Third-Party Systems: The architecture must allow connecting to other external systems through secure APIs. Aside from insurance and inspection systems detailed earlier, consider possible integration with:

١.١٢.٤. Customs System: to validate customs clearance for vehicle imports.

١.١٢.٥. Traffic Court System: if fines disputes or court decisions about violations need to reflect in the record.

١.١٢.٦. Postal/Delivery Services:

If the system will support delivering documents (like if registration cards or plates can be mailed, the system might integrate with a courier to track deliveries).

١.١٢.٧. Directorate General of Personal Status (Civil Registry): identity, family status and vital events validation for applicants and vehicle owners.

١.١٢.٨. Ministry of Social Affairs: verification of disability status and special-needs entitlements for persons with disabilities, to support eligibility for fee exemptions, special plates/parking privileges, and any other benefits defined by the Authority.

١.١٢.٩. Commercial Registry & Chambers of Commerce, Industry and Agriculture: company registration/extract validation for corporate owners and professional transport licensing.

١.١٢.١٠. Ministry of Industry: verification of industrial operator status where required for commercial vehicle categories.

١.١٢.١١. SMS, whatsapp and Email Gateways: for sending notifications and OTPs (one-time passwords) to users.

١.١٢.١٢. Central e-Government Portals: If the government has a one-stop portal for services, the system shall provide necessary hooks or web services to be accessed through such a portal.

١.١٢.١٣. DGGS (General Directorate of General Security) integration: Validate foreign nationals' identity, residency/visa, and entry/exit constraints through DGGS services; apply configurable hard-stops when violations or bans are returned.

١.١٢.١٤. Judicial& security registries: Where lawful, query judicial/criminal record services for required certificates (e.g. "Sijil Adli") and receive watchlist events; event hooks trigger holds and notifications with full audit.

١.١٢.١٥. Sectoral Permit Verification — Rokhas Nakel (Transport Permits), Ministry of Industry (MoI), Ministry of Agriculture (MoA), and other competent authorities designated by the Authority

- Scope. For services/vehicle classes that require sectoral authorization (e.g., public/commercial cargo, agricultural machinery, industrial logistics), the Platform SHALL verify required permits with Rokhas Nakel, MoI, MoA, and any additional competent authorities added by configuration—no code changes.
- Interfaces. Verify by UTN/plate/VIN/permit number and retrieve current status (valid/expired/suspended) and permit attributes needed for decisioning.
- Service Gating. Registration, renewal, transfer, and NOC flows SHALL hard-stop if a required permit is missing/expired/ineligible; holds lift automatically when status is cleared.
- Evidence & Audit. Store permit reference(s), returned status, and supporting documents; display permit status on the case/vehicle record.
- Configuration. Back-office screens SHALL map which services and vehicle classes require which authority checks and define any fee splits per §١.٢٥.١٢.

١.١٣. Data Migration and Legacy Support: The vendor must account for migrating all existing data from the legacy systems (current system and any other databases used by AUTHORITY) to the new system. This includes vehicle records, driver records, transaction history, archived

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

documents, and any external data needed). The new system shall also ensure continuity of service: during the transition period, it may need to run in parallel with the legacy system or at least ensure data consistency if cut-over is staged (for example, a period during which new transactions happen on the new system while old ones are being closed out). The migration shall handle data cleansing (eliminating duplicates, correcting errors where possible) and proper mapping of old fields to new fields. A complete migrated dataset is critical so that historical information is not lost and users do not have to access two systems.

٥. SYSTEM COMPONENTS – SOFTWARE AND APPLICATIONS

١.١٤. The solution shall include a dedicated, complete, and proper Legacy Data Migration & Reconciliation Service—covering discovery/profiling, ETL/ELT mappings, deduplication to the UTF, document/media ingest, rehearsal runs in staging, reconciliation reporting, secure cutover and rollback—to transfer all required data from current systems into the new platform.

١.١٥. All discovery/profiling, ETL/ELT, staging, reconciliation and cutover activities— including any temporary working copies—shall be executed strictly on Authority premises under Authority custody; no production or legacy records may be exported off-site.

١.١٦. The proposed system must be an integrated platform comprising all necessary software modules and applications to serve each department and branch office of the Authority.

٦. USER REQUIREMENTS

The system shall serve a wide range of user groups. Each group's requirements must be addressed to ensure usability, inclusivity, and compliance with Authority standards.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

User Group	Privileges / Access
Citizens	Access services through the portal and mobile app to renew registrations and licenses, pay fines, schedule appointments, receive notifications, and obtain digital or physical credentials.
Stakeholders (Notaries, driving schools, physicians, …)	Secure access to perform role-specific tasks, such as ownership transfers, exam scheduling and results, and submission of medical fitness certificates. Transactions are limited to their domain and fully auditable.
Authority Staff	Role-based access to back-office functions, including transaction processing, approvals, system configuration, reporting, and monitoring, with audit logging and supervisory controls.
External Agencies (Law enforcement, MoF, Customs, …)	Controlled access through secure interfaces to query and update relevant records (e.g. fines, customs clearance, residency checks, insurance verification) strictly within their authorized scope.

٧. FUNCTIONAL REQUIREMENTS (BY MODULE)

This section details the specific business processes and services that must be automated and supported by the new system. The aim is to digitize the entire workflow of the Traffic and Vehicle Management Authority services, eliminating manual steps and integrating all requirements so services can be delivered efficiently both online and in person.

١.١٧. Vehicle Registration Management Module:

To handle all vehicle-related services, including new registrations, renewals, transfers of ownership (sale or other title changes), import/export of vehicles, deregistration (vehicle retirement), and issuance of related documents (registration cards, license plates, etc.). This module shall maintain a unified vehicle record for each vehicle, identified by a unique Vehicle Identifier, and track its status, inspection validity, insurance, outstanding fines, etc.

١.١٧.١. Vehicle Type Approval & Controlled Modifications

- Maintain a Type Approval Registry (make/model/variant)
- Manage controlled modifications (color/engine/capacity/usage) tied to inspection and e-NOC.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

- Block completion of registration changes until inspection pass and approvals are recorded.

١.١٧.٢. Lifecycle States & Rules:

- Define explicit states: Active, Exported, Scrapped, Salvage/Write-off, Rebuilt.
- Configure allowed services per state and maintain an audit trail of state changes (who/when/why, supporting documents).
- Enforce VIN/plate status checks before any service.
- Provide 'Suspended from Circulation' and 'Reinstated' administrative statuses with certificates and service gating; all transitions are audited.

١.١٧.٣. Lien/ Vehicle Mortgage Management:

- Provide an end-to-end lien lifecycle with a secure Banks/Lenders Portal and APIs to create, amend, renew and release liens.
- While active, liens shall automatically block transfer/export/scrap. Upon release, the system generates a digitally signed e-NOC.
- All steps are logged with time stamps, user IDs and attachments.
- Rules (e.g. renewal blocks, cooling-off windows) shall be configurable.

١.١٧.٤. No-Objection Certificates (NOCs):

- Implement configurable e-NOC workflows for sale, export, color change, engine change, plate change, salvage/write-off and rebuild.
- Support digital signatures (qualified where available), PDF output with QR validation.
- Service blocking until required NOCs are issued/closed.
- All NOC artifacts shall be retained per records policy.

١.١٧.٥. Vehicle Registration Services:

- **New Vehicle Registration (First-time Registration):**

  Ability to register a newly imported or manufactured vehicle. This process involves capturing vehicle details (make, model, year, chassis/VIN, engine number, etc.), owner information, and required documents (customs clearance for imports, purchase invoice, etc.). The system shall generate a new registration record, assign a unique plate number (unless a special number is being assigned), calculate and collect the necessary fees/taxes, and issue the registration card, license plates, and sticker (if applicable). If any pre-requisites are required by law (e.g. inspection for used imports, or ensuring the owner has a valid driver's license), the system must enforce those rules.

- **Annual Registration Renewal (Mechanique):**

  A workflow for yearly renewal of vehicle registration. The system shall check that all

preconditions are met before allowing renewal (Inspection checks are policy-driven and may be toggled per vehicle class/period if the national program is paused/resumed.): valid periodic mechanical inspection, valid insurance policy, and no outstanding fines or penalties on the vehicle or owner. A step-by-step wizard will guide the user or clerk: (١) Verify insurance (system fetches or validates insurance status); (٢) Verify inspection pass (from inspection data); (٣) Check for unpaid fines and optionally allow payment of fines on the spot; (٤) Then allow renewal fee payment. Only when all conditions are satisfied can the registration be renewed, also any other step not mentioned could be added by the Authority.

- **Registration Card Issuance & Renewal Policy:**

  By default, the Authority does not operate a renewal process for the physical vehicle registration card. One physical card is issued at initial registration and remains valid until deregistration or transfer of ownership; reprints occur only upon core-data changes, loss/damage, or an Authority-mandated security refresh. Renewal of registration status (if any) is reflected digitally in the system/portal/app and remains roadside-verifiable via QR/UTN.

- **Activation by Request Only (Annual Renewal Mode):**

  If—and only if—the Administration formally requests introduction of a renewal regime, an Annual Renewal Mode shall be activated by Back-Office configuration (no code changes) with maker-checker approval and full audit of who/when/why. When activated, each annual renewal updates the digital status; and physical card is produced only if the citizen explicitly requests a physical card. Deactivation restores the default (no card renewal).

- **Transition & Outputs:**

  When Annual Renewal Mode is active, existing one-time cards remain valid until the next applicable renewal; at that event, the prior card is invalidated only when a citizen-requested physical reprint is issued, otherwise the existing physical card remains and only the digital status is updated. The output of renewal is an updated registration validity date in the system, a new electronic sticker issued if physical stickers are in practice, and a digital confirmation sent to the owner. Late fees and penalties are applied automatically per regulations.

- **Transfer of Ownership (Vehicle Sale/Purchase):**

  Digitize the process of selling a vehicle and transferring the title to a new owner. This includes capturing the sale request (initiated by seller or buyer), involvement of a notary

public to legally endorse the sale, and updating the ownership in the system. The system shall support both immediate title transfer (where buyer and seller come to the Authority or a service center with a notarized sale contract) and Power of Attorney based transfer (where initially a PoA is used to allow the buyer to use the vehicle and the official transfer happens later). In all cases, the system must ensure any required fees (transfer fees, PoA fees, accumulated annual fees if the registration is out of date, etc.) are calculated and collected. After transfer, the vehicle's record is updated with the new owner's details, and new registration documents (card, plates if number changes or new series) are issued to the new owner. The old owner's record shall reflect that they no longer own the vehicle. All historical ownership data shall be retained.

- **Vehicle Deregistration (Write-off or Export):**
  Process for removing a vehicle from the active registry. This could be due to the vehicle being scrapped (destroyed), permanently exported to another country, or otherwise taken off the road. The system shall guide the required steps (e.g. surrendering plates, issuing a certificate of deregistration) and mark the vehicle record as inactive/archived. If the vehicle is being exported, the system might issue export documents and allow customs to verify them. Any outstanding obligations (unpaid fines, fees) must be settled before deregistration.
- **Duplicate or Replacement Documents:**
  If an owner needs a duplicate registration card (because of loss or damage) or a replacement sticker/plate, the system shall facilitate issuing replacements. It shall verify the request (e.g. requiring a police report for lost items if mandated), collect any replacement fees, and then issue the new document, marking the old one as void. The system shall prevent misuse (like multiple active registration cards) by invalidating previous documents and updating the record.
- **Temporary Plates (Law ٢٤٣/٢٠١٢, Arts. ١٤٧–١٥٠):**
  The system shall issue and manage: (i) Agent Temporary Registration/Driving Plates (Art. ١٤٧); (ii) Temporary Import Plates (Art. ١٤٨); (iii) Test Plates (Art. ١٤٩); and (iv) Transit Plates for export/movement (Art. ١٥٠). Each category must have configurable validity windows and fees, QR for roadside verification, automatic expiry, and misuse controls that trigger renewal/service blocks per policy.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

- **Additional Vehicle Categories:**

  The Platform shall fully support registration, renewal, transfer, and deregistration for:

  i. motorcycles, mopeds, scooters, and trikes with engine-capacity/kW classes;
  ii. trailers and semi-trailers, including VIN assignment for homebuilt/kit trailers;
  iii. agricultural and construction equipment (tractors, harvesters, backhoes), ATVs/UTVs, and off-road vehicles where road-permitted; when applicable, enforce sectoral permit validation per §١.١٢.١٤.
  iv. vintage/collector/classic vehicles under limited-use permits; and
  v. electric and alternative-fuel vehicles (EV/HEV/PHEV/LPG/CNG).

  Category-specific rules (fees, inspection/emissions, exemptions, usage limits) shall be configurable and enforced by the service engine.

- **Tanker Sub-classes:**

  Define tanker sub-classes (water, fuel, hazardous) with mandatory safety certificates, periodic inspections, and policy-based exceptions where applicable.

- **Public/Commercial Cargo Vehicles:**

  Define a "Public/Commercial Cargo Vehicle" category with distinct tariffs, inspection requirements, route/usage restrictions, and renewal workflows covering Lebanese vehicles, used foreign imports, and new foreign (٠ km) vehicles.

- **Public/Tourism Vehicles:**

  Define a "Public/Tourism Vehicle" category with dedicated fees, inspection/insurance rules, and issuance/renewal workflows for both Lebanese and foreign vehicles.

- **Special Owner Categories:**

  Model special owner categories (e.g. judiciary, parliament, ministries, persons with disabilities, religious courts) with configurable entitlements (fees, exemptions, plate formats) and eligibility checks.

- **Special Construction & Rebuilds:**

  Support approvals and workflows for rebuilds/kit cars, flood/salvage branding, axle/body-type changes, and engine/chassis swaps. Enforce pre-issuance inspection/e-NOC, re-inspection on return-to-road, and branded titles (Salvage/Rebuilt) with full audit.

- **VIN Assignment & Corrections:**

  Provide VIN assignment for VIN-less vehicles/trailers, police-forensics-driven VIN corrections, and re-stamping approvals; all events shall be versioned with chain-of-custody.

- **Vehicle Occurrences/History Certificate:**

  Generate a digitally signed Vehicle History Certificate (ownership chain, legal holds/seizures, liens, and other occurrences) as a QR-verifiable PDF attached to the vehicle record. System must capture and audit owner consent before issuance; bypass permitted only for authenticated Authority accounts with statutory basis recorded in the request log.

- Sectoral Permit Check (Rokhas Nakel/MoI/MoA/other designated authorities): Enforce verification per §١.١٢.١٤ and block issuance/renewal/transfer until valid.

١.١٧.٦. **Distinguished Plate Numbers Management:**

The system shall incorporate the management of special or distinctive license plate numbers. This includes:

- **Special Number Retention & Transplant:**
  - Allow owners to retain a number independent of a vehicle (for a fee) and transplant retained numbers between owned vehicles subject to policy checks and e-NOC.
  - Enforce holds/annual retention fees and block conflicting services until dues are settled.
- **Premium Plate Registry:**
  - Maintaining a registry of premium number plates (e.g. repeating digits, unique sequences) that can be sold or auctioned to the public for additional fees.
- **Enforcement of Rules:**
  - Enforcing rules for these plates as defined by the Authority (for example, a special plate might carry an initial purchase cost and possibly an annual fee for retaining it).
  - The system shall be able to levy that annual fee and link it to the registration renewal of that vehicle number.
- **Transfer of ownership:**
  - Allowing the transfer of a distinctive plate from one vehicle to another (when the owner changes vehicles) according to policy, including collection of any transfer fees or approval steps required.
- **Auctions & reservations:**
  - Provide a full auction engine (English/Arabic/French and sealed-bid) with bidder registration, deposits, anti-collusion controls, and award workflows.

- Support reservation of a premium number independent of a vehicle, with issuance of a digitally signed Certificate of Allocation; allow annual retention/holding fees until assignment.

- **Document chain & history:**
  - Manage the complete document set (allocation certificate, auction records, transfer deeds) in DMS with full lifecycle logs(who/when/what), versioning, and tamper-evident audit.
- **Monetization & rules:**
  - Enforce policy rules (initial purchase, annual retention, transfer fees) and block conflicting services until dues are settled.
  - Expose APIs for public catalogues and results.

١.١٧.٧. Requirements for Electronic Vehicle Registration Cards

Authority Visual Design and Branding. The card shall continue with the current Authority-approved visual design and branding. Bidders shall reproduce the present layout, colors, emblems, and bilingual text exactly as currently issued, subject only to Authority-mandated security-feature refreshes (e.g. hologram/DOVID patterns, microtext) that do not change the visual layout. No redesign is permitted unless the Authority provides prior written approval and approves physical samples.

If the card's validity is one year and it is reissued annually, there might be color coding by year or a prominently displayed expiration year to easily see if it's expired. Alternatively, if the card is not replaced annually, the card could be more permanent and the actual validation of renewal is done via the electronic system or sticker. (This is a policy decision).

Link with Electronic Stickers: The registration card shall be designed to complement the use of the vehicle sticker. The card is something the owner keeps (and might need to present in certain situations, like selling the car or out-of-country travel), whereas the sticker on the vehicle serves as quick proof of valid registration to authorities. Data on both shall match. Possibly the card could have the same identifier as the sticker (for instance, the sticker's RFID code or serial is printed on the card for cross-reference).

Validity and Renewal Mechanism. By default, the registration card is one-time (multi-year) and remains valid until deregistration or ownership transfer. Annual renewal—when applicable—updates the vehicle's digital status only (portal/app; QR/UTN roadside-

verifiable). No physical reprint occurs except for core-data change, loss/damage, or an Authority-mandated security refresh.

If the Administration activates Annual Renewal Mode each renewal updates the digital status and optionally produces a new physical card only upon citizen request. When a new card is issued, the prior card is automatically invalidated; if no card is requested, the previous physical card remains and the renewed status is reflected digitally.

Issuance events (whether default or Annual Renewal Mode) synchronize with e-sticker workflows when stickers are in practice, apply late fees per tariff rules, and generate digital confirmations/receipts. No mandatory mass card printing is required; capacity planning covers reprints and citizen-requested cards only.

Overall, the electronic vehicle registration card will serve as the official document proving vehicle registration, much like the driving license does for driving privileges. It shall be secure and integrate with the digital system, thereby reducing fraud (like forged car papers) and simplifying law enforcement verification.

١.١٧.٨. Requirements for the Vehicle Registration Issuance System

- Card Printing Equipment: The vendor shall provide if not present card printers dedicated to vehicle registration cards.
- Printers shall be capable of the security overlays.
- Issuance Locations: Deploy registration-card issuance software/hardware at branch offices and designated installation centers; enforce inventory control and chain-of-custody for blanks and produced cards.
- Quality Assurance: As with licenses, ensure correctness.
  The card's printed plate number, etc., must correspond to the vehicle.
  Faulty prints (misprints) shall be logged and reprinted. Because renewals might be high-volume, the system shall minimize errors by maybe printing a test batch for calibration each day.
- Handling of Lost or New Cards: If a vehicle owner replaces a lost registration card, the system shall mark the old card as void and trigger printing of a new one (with possibly a "duplicate" notation if needed). The issuance system shall handle these on-demand prints as well.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

- Blank Card Stock and Inventory: Blank vehicle card stock shall also be managed, they shall be tracked separately. Inventory management for these blanks is required as well, per location. The security of blanks is equally important.
- User Operation and Training: Staff at branches will need to operate these printers. The interface shall be simple: a print queue showing pending cards and status. Staff can initiate reprints if needed. The vendor shall train the staff on operating and maintaining these printers (very similar to license card printer training).
- Electronic Delivery: one might consider not issuing physical cards at all and relying on digital proof. However, until law fully recognizes digital-only, physical cards remain necessary. The system shall be flexible such that if in future the Authority decides to stop issuing physical registration cards (relying on online verification), the printing can be phased out. This is just to ensure no lock-in to always print if not needed – but currently it is required.

In essence, ensures that every vehicle's registration certificate can be securely and efficiently produced by the system, complementing the digital records with a tangible document for the owner.

١.١٨. **Driver Licensing Management Module:**

To manage the issuance of driving licenses and permits. It shall cover driver records (profile with personal details and unique ID, e.g. national ID number), applications for new licenses, scheduling and recording of theory and practical driving exams, issuance of new licenses, renewals, upgrades (adding categories), suspensions/withdrawals (e.g. due to violations or point system), and replacements for lost or damaged licenses. A unified driver profile shall link each person's license data, driving history, violations, and points.

١.١٨.١. **Issuance of New Driving License (Learner and Full):**

Manage the end-to-end process from license application to issuance. This involves capturing applicant information (personal data, photos, signature, biometric data, fingerprints+ face), conducting theory and practical exams, and finally issuing the license. The system shall allow driving schools or applicants to apply and schedule tests online. The testing officers (examiners) can input the results (pass/fail, scores) directly into the system. If an applicant passes all required tests and meets age/medical criteria, the system will permit license issuance: it will assign a license number, determine the class of license and its validity period (the exact durations per category shall be configurable as per Lebanese traffic law), and prompt for fee payment (including any stamp duties or training fees). After

payment, the license card is produced. The system shall also handle adding endorsements (like if they are also a public transport driver requiring additional permissions).

١.١٨.٢. License Renewal:

Process for renewing a driving license upon expiry. The system shall notify license holders in advance of expiration (via SMS/email/through the portal/mobile app notification). Renewal may require certain conditions depending on category – for example, possibly a medical fitness certificate for senior drivers or for heavy vehicle categories, or an eye test. Where remote medical certification is permitted, the renewal workflow SHALL accept physician submissions captured with liveness per §١.٣٩.٢; renewal is blocked if the liveness score is below the Authority-set threshold or the certificate is invalid/expired. The system shall enforce submission of any such requirements by providing interfaces for authorized entities (e.g. a medical practitioner or an official at a testing center) to input their approval. It shall also check for any unpaid traffic fines by the applicant, as renewal might be blocked if fines are outstanding (subject to policy). Once conditions are met, the applicant can pay the renewal fee and the system will extend the license validity and issue a new license card. The old license status becomes expired in the record. Configurable photo-refresh policy. When enabled, a new driver photo is required as a prerequisite for renewal every X years (configurable interval), with effectiveFrom and gracePeriod parameters set by the Authority.

١.١٨.٣. License Replacement and Modifications:

In case of lost or damaged license, the system shall allow for issuing a replacement (after verification of identity and a police report for lost license). If a license holder needs to update information (e.g. change of name or address), the system shall handle these modifications as allowed by policy, possibly issuing an updated card. If upgrading a license category (e.g. obtaining a higher class to drive trucks, or adding a motorcycle class), the system must handle the application for an upgrade, ensure the required tests are taken, and then issue a new license reflecting the new classes.

١.١٨.٤. Point System and Violations Impact:

The licensing module must be tightly integrated with violations. For instance, if the law prescribes automatic suspension of the license at a certain point threshold, the system shall flag the license as suspended once that threshold is reached, and trigger any required workflow (like scheduling a retraining or test after suspension). It shall also be able to reinstate licenses after suspension period or after conditions are met (e.g. points reset after a year of no violations, depending on the law).

١.١٨.٥. **International Permits and Exchange:**

If the Authority issues international driving permits (IDP) or handles exchange of foreign licenses, these processes shall be digitized as well. For example, recording an exchange of a foreign license for a Lebanese one (and ensuring one person does not hold multiple valid licenses in Lebanon), printing of International Driving Permit booklets, etc., with fees and issuance tracked.

١.١٨.٦. **Conversion of licenses:**

Support conversion of military driver licenses to civilian classes with validation of military records and configurable equivalency rules.

١.١٨.٧. **Social Security (NSSF) Attestations:**

Integrate with Social Security to Support verification, and attachment of NSSF attestations/clearances required for commercial passenger, freight, and public bus categories.

١.١٨.٨. **Computer-Based Theory Tests:**

Deliver an question bank with randomization, Arabic/English/french (and accessibility options), configurable scoring, and optional remote proctoring (live or AI-assisted). Publish result APIs back to Licensing and schools.

١.١٨.٩. **Exam Committee Field App & Results Orchestration:**

Provide an examiner/committee tablet app (iOS/Android) bound to per-device certificates that works online/offline to capture practical test results using standardized rubrics. Each submission shall include time/GPS stamps and optional photo/video evidence where policy permits. Results flow to a maker-checker workflow for supervisory approval; only approved results update the applicant's UTF and licensing record. All steps are fully audit-logged (who/when/where/device) with immutable logs, and the system shall automatically compute examiner compensation per approved test using a configurable rate matrix, generating period settlements and finance-ready payout files.

١.١٨.١٠. **Instructor/Examiner Accountability & Anti-Tamper Controls:**

The system shall maintain tamper-evident counts and KPIs per driving-school instructor and per examiner/committee member, including unique candidates tested/taught, attempts, pass/fail rates, test durations, cancellations/no-shows, and route adherence. Assignments must originate from scheduled appointments; device+user identities are enforced; post-submission edits are disallowed except via supervised correction flows with dual-control

approval. Anomaly detection (e.g. outlier pass rates, abnormally short tests, geofence violations) raises review tasks and reports.

١.١٨.١١. **Auto-Notification & Digital License Provisioning:**

Upon approved pass and fee settlement, the service engine shall (i) push SMS/app/email notifications to the applicant with result and next steps; and (ii) automatically provision the digital driving license to the citizen's mobile app wallet (per Mobile App & Digital Credential Security), while queuing physical card personalization as per issuance policy.

١.١٨.١٢. **Requirements for Electronic Driving Licenses**

Authority Visual Design and Branding. The card shall continue with the current Authority-approved visual design and branding. Bidders shall reproduce the present layout, colors, emblems, and bilingual text exactly as currently issued, subject only to Authority-mandated security-feature refreshes (e.g. hologram/DOVID patterns, microtext) that do not change the visual layout. No redesign is permitted unless the Authority provides prior written approval and approves physical samples.

Digital Driver's License: the system design shall also consider the digital driver's license concept. The system shall be able to generate a digital representation of the license for use in a mobile app or wallet, with a QR code or similar, so that citizens can carry their license electronically. This digital license would complement the physical card and shall have equivalent information and security (digital signatures for verification). Bidders can outline how their solution accommodates this (even if full implementation of a mobile license might be a later phase).

In summary, the new driving license must be a secure, smart card that significantly enhances trust and functionality. It will serve as an authoritative ID for drivers and must be difficult to forge, easy for authorities to verify (both by eye and electronically), and integrated with the system's database for real-time status checks.

١.١٨.١٣. **Requirements for the Driving License Issuance System**

To produce and personalize the smart driving license cards, the solution must include a complete issuance subsystem. This encompasses the hardware for card printing and encoding, the software that manages card personalization, and the processes around issuance. Key requirements are as follows:

- Card Personalization Equipment: The vendor shall provide if not present the necessary card printers/encoders that can handle the chosen license card technology. Depending on the present design form, this could include:

- High-resolution card printers capable of printing color photos, graphics, and overlay features. If using polycarbonate with laser engraving, then laser engraving machines will be needed instead (these engrave the card rather than print with ink).
- The printers must include an RFID encoder unit to program the chip during the printing process.
- The equipment shall support applying holographic overlays or laminates if those are separate steps (some printers have lamination modules).
- The throughput of the printers shall meet the demand,. Bidders shall state printing speed (cards per hour) and number of machines proposed per site to ensure no bottleneck.
- Redundancy: at least two printers at main centers so that if one fails, issuance can continue. Also, maintenance kits and spare parts shall be included.
- Enrollment Devices: For capturing the data that goes onto the license, the system shall include:
- Digital Cameras for capturing applicant photographs at a high resolution .The system shall enforce that photo capture meets required criteria (size, lighting, no smile, etc. as per regulations).
- Signature Pads or Tablets to capture the applicant's signature digitally, which will be printed on the card and stored in the system.
- Biometric Enrollment Devices (Existing; Supply-on-Request). The Authority already operates biometric kits capable of fingerprint capture and live photo capture. The SI shall integrate with these existing devices (reuse current models/SDKs), provide drivers and middleware, and certify end-to-end compatibility with the issuance workflow (photo → fingerprints → signature → data verification → print). The SI shall maintain and support the existing kits (calibration, firmware, troubleshooting) and keep spare parts/consumables. Additional units shall be supplied only upon written request of the Administration, matching approved makes/models or Authority-approved equivalents. All enrollments must meet target throughput (≤٥ minutes per applicant) and quality thresholds (auto quality checks, retry prompts), with full audit of device ID, operator, time, and station.

١.١٨.١٤. **Enrollment Performance:**

The end-to-end data capture and enrollment step shall not exceed ٥ minutes per application under normal operating conditions. Expose per-device and per-user KPIs (average handling time, throughput) on operational dashboards.

١.١٨.١٥. Driver Registration Data Model:

Capture and store (subject to change by Authority) the following data elements with bilingual support where applicable: full name in Arabic and Latin scripts; date and place of birth; parents' names; nationality; categories authorized; issuing officer code; license usage (private/public; automatic where applicable); phone; residential address; blood type (if permitted); restrictions/medical accommodations (persons with disabilities); signature image; photo; national ID number; and any other Authority–mandated attributes. Allow Latin transliteration input and store both scripts in the data model.

١.١٨.١٦. Issuance Software Workflow:

The card issuance system shall be integrated with the main application. Typically, once an applicant is approved for license issuance (all exams passed, fees paid, etc.), the system flags that a license card can be issued. The issuance software then:

- Retrieves the personal data and photo/signature from the database.
- Encodes the chip with the data (securely).
- Personalizes the card print: placing text, photo, signature, and security features accordingly.
- Prints/engraves the card and then verifies that encoding was successful (for example, reading the chip or barcode to ensure data matches the record).
- Marks the record as "card issued" with the issuance date and card serial number in the database.

This process shall be largely automated to reduce manual data entry. The operator's role is mainly to load blank cards, initiate the print job for each approved applicant, and verify the output quality.

١.١٨.١٧. Quality Control and Reissuance Handling:

The system shall implement checks to ensure the right card is given to the right person:

- Ideally, after printing, the operator could scan the card (via chip or barcode) and the system will pull up the corresponding record to confirm it matches the intended person, as a final check.
- If a card is misprinted or fails encoding, the system shall allow re–printing. The spoiled card must be logged (with its serial number) as destroyed to maintain inventory control.
- If a person does not show up to collect their license, the system shall record that the card is in inventory at the office, awaiting pickup. It shall also allow cancellation if not picked up after a certain time, per policy.

١.١٨.١٨. **Card Inventory Management:**

The vendor must supply license cards, and the system shall track the inventory of these:

- Each card may have a batch number or unique ID which can be scanned (if manufacturer provides). The system shall decrement inventory as cards are used.
- Alerts for low stock at each location shall be generated so new stock can be ordered in time.
- Secure storage: cards are sensitive assets; the system admin module shall record which user took cards into production, etc. Some manual processes (like physical log books) may complement this, but the system can at least record usage counts per user.

١.١٨.١٩. **During issuance:**

If fingerprint verification is required before issuing (to ensure the person is who they claim or that one person doesn't get multiple licenses under different names), the issuance workflow shall include sending the captured fingerprint to the central system and receiving a confirmation or an ID match. The issuance would proceed only if the system returns an OK (no duplicate or issue). This must be done relatively quickly (within minutes) to not stall the applicant's processing.

١.١٨.٢٠. **Printing of Temporary Licenses or Receipts:**

A temporary paper license (or receipt) is to be given until the card is produced. The system shall allow printing a temporary driving permit (with limited validity) if needed – for example, in case the card printer is down or if licenses are issued centrally and mailed, a person might get a temp license immediately. This document shall have a unique identifier and be logged, and automatically expire as per rules.

١.١٨.٢١. **Decentralized Issuance:**

The system shall support decentralized (likely the case for efficiency), ensure each branch has needed printers and the system synchronizes data so that one person cannot attempt to print at two places (not likely if one record).

Also, consider future involvement of private centers – if in long term some private offices are allowed to issue licenses, what safe guards are needed (they might print under supervision or maybe still only branches can print cards for security).

١.١٨.٢٢. **Maintenance of Issuance System:**

The vendor will be responsible for maintaining the card printers and related equipment. This includes periodic cleaning, part replacement (print heads, etc.), and software updates for printer firmware. The RFP shall require a certain minimum up time for the issuance equipment and a support plan (e.g. faulty printer replaced or repaired within ٤٨ hours so that

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

service is not disrupted). Training must be given to staff on basic troubleshooting (like clearing card jams, replacing ribbon or laminate, etc.).

Overall, the driving license issuance system is a critical component that turns digital approvals into a secure physical credential for citizens. The bidders must provide a detailed description of the make/model of printers and enrollment devices, their capacity, and how their solution ensures quick and secure issuance of licenses with minimal errors.

١.١٩. **Unified Traffic File (UTF) Module:**

١.١٩.١. The Contractor shall implement a single **Unified Traffic File** per person/entity serving as the system-of-record key across Vehicles, Driver Licenses, Violations, Points, Liens, Impounds and Services.

١.١٩.٢. UTF shall:

- Expose a UTF ID used as the primary key across internal services and partner APIs; Issuance & Backfill. A UTN is minted at the first lawful registration of a Person/Legal Entity or Vehicle; all subsequent services reference the same UTN. Legacy datasets shall be backfilled via a UTN Alias Map (legacy IDs → UTN) managed on-prem. Any merges keep the survivor UTN and preserve merged UTNs as immutable aliases; splits allocate new UTNs with full audit, leaving the original UTN as historical only.
- Include deterministic and probabilistic deduplication (fuzzy matching on name, national ID/passport, mobile, email);
- Provide merge/split workflows with full audit; and
- Support ٣٦٠° views (persons, companies, fleets) in line with applicable Lebanese law.

١.٢٠. **Enforcement and Violations Module:**

١.٢٠.١. Traffic violations:

To record and manage traffic violations, fines, and a points system. This includes integrating with law enforcement inputs – e.g. allowing police officers to query vehicle and driver information roadside (via a secure mobile app or handheld device) and to issue e-tickets/violations that automatically register in the system against the driver's profile. The module shall support a points-based license system (tracking demerit points per driver and triggering warnings or automatic suspensions as per Lebanese traffic law). It must also handle fine payments and update license/registration status (for example, preventing renewal if fines are unpaid or if points threshold is exceeded).

١.٢٠.٢. Impound and Legal Holds:

Provide yard intake/release, impound fees, storage accruals, and inventory (photos, location, condition). Manage court/police blocks, export/travel bans, and stolen flags received via

secure interfaces. The service engine must respect active blocks (hard-stops with reason codes) and log all override attempts with maker-checker approval.

١.٢٠.٣. Stolen/Recovery Feeds:

Integrate with police systems to auto-flag stolen vehicles and apply hard service blocks until recovery/closure is received. All events are versioned and auditable.

١.٢٠.٤. Municipal Parking & Other Liabilities:

Ingest municipal parking violations/unpaid fees (and future toll/ANPR sources); expose them in renewal/issuance workflows; support disputes, unified settlement, and reconciliation back to municipalities.

١.٢٠.٥. Judicial & Insolvency Orders:

Ingest and execute court-ordered holds/unholds, travel bans, and bankruptcy/liquidation asset freezes, reason codes, and automatic service blocking until lawful release is received; all overrides require maker-checker approval.

١.٢٠.٦. Traffic Fines and Enforcement:

Every violation (fine) issued to a vehicle or driver shall be recorded in the central system (either entered by police through their interface or via data migration from legacy systems). The system must:

- Link fines either to a vehicle (if it's a camera or plate-based violation) or to a driver (if a license was presented).
- Prevent certain services until fines are paid (for instance, registration renewal or license renewal cannot proceed if there are unpaid fines on that vehicle or driver, unless an override by authorized personnel is used for exceptional cases).
- Provide a citizen the ability to view and pay their fines online. Upon payment, the system updates the status to paid and reflects in the driver/vehicle record.
- Update point totals on the driver's license if the violation carries point deductions.
- If a court or other Authority orders a fine cancellation or adjustment, the system shall allow administrative editing of a fine record by authorized officials with proper logging.
- In addition, the system could integrate with any existing e-challan or traffic camera systems that generate violations, so that data flows automatically.

١.٢١. **Vehicle Inspection Integration Module:**

١.٢١.١. To integrate with authorized vehicle inspection centers. It will receive inspection results (pass/fail and details) for each vehicle via API in real-time. The system must mark a vehicle as eligible for renewal only if a valid inspection pass record is present (as required by law).

This module shall accommodate both government-run and licensed private inspection centers as part of a future decentralized model. It shall allow registration of multiple inspection centers, each with secure access to update inspection results, and time stamp and log each entry. Historical inspection data shall be stored in the vehicle's record. (If the mandatory inspection program is paused or resumed, the system's business rules for requiring inspection shall be configurable.)

١.٢١.٢. Recall/Safety Bulletins. Ingest recall feeds from manufacturers/regulators. Optionally block renewal until mandatory recalls are resolved; capture proof during inspection (work order/receipt images). Maintain VIN-level recall history.

١.٢١.٣. Center Governance. Provide licensing criteria, readiness checklists, digital QA scoring, penalties/escalations, and automated SLA dashboards per center. Include a roaming-inspector app and audit trails.

١.٢١.٤. Vehicle Inspection Process: Although vehicle inspections (mechanical fitness tests) may be conducted by external centers, the system must enforce their role in registration workflows. This means:

- Each vehicle record shall store the inspection schedule (e.g. new vehicles might be exempt for a certain number of years, others require annual inspection depending on vehicle age/type as per regulations).
- The system will receive results from inspection centers via the integration module. If a vehicle fails inspection, the renewal process shall be halted or flagged until a pass is recorded.
- The system shall be able to generate or accept an inspection appointment if scheduling is needed (if the new system will also allow citizens to book inspection slots online at approved centers).
- Support auditing of inspection results (for example, statistical reports on pass/fail rates per center, to identify any anomalies).

١.٢٢. **Insurance Integration Module:**

To ensure no vehicle is registered without valid insurance, the system shall interface with insurance companies. An Insurance Verification Portal/API will allow insurance providers to update the system with insurance policy status for each vehicle (or allow the system to query insurance databases). Before a vehicle's registration is renewed, the system must check that an active insurance policy exists. This module shall store basic insurance info (company, policy number,

validity dates) in the vehicle record. It shall also allow for different workflows for foreign or transit vehicles, if applicable, and verify insurance for those as needed.

١.٢٣. **Notary and Legal Processes Module:**

Needed for handling the legal formalities of vehicle sales and transfers.

١.٢٣.١. Notaries (public notaries) shall have a dedicated portal or secure access to the system to electronically certify and approve ownership transfers and other legal documents (e.g. inheritance transfers, power-of-attorney notifications for vehicle use or sale).

١.٢٣.٢. The module shall manage ownership-transfer workflows requiring a notary's approval and signature. Until digital (PKI) signatures are legally recognized, the system shall capture the notary's handwritten electronic signature on a signature pad and bind it to the transaction record. Where and when digital signatures are legally recognized, the module shall support PKI-based digital signatures. The signature method shall be configurable by jurisdiction and enforced before finalization.

It must also integrate with any external systems or databases needed (for example, the Syndicate of Notaries or a national e-signature service) to verify notary credentials .

١.٢٣.٣. In addition, the system shall capture Power of Attorney (Wakalat) transactions: if a vehicle is sold via a notarized power of attorney without immediate title transfer, the system shall record this event, flag the vehicle record (e.g. "under PoA sale"), and ensure that proper fees or taxes associated with such transactions are applied when the actual transfer occurs.

١.٢٣.٤. Citizen signature capture: Notary and front-office flows must include signature pad capture for citizen/representative signatures, embedded into the transaction artifacts and archived in DMS.

١.٢٣.٥. Qualified e-signature: Notaries shall apply a qualified electronic signature (PKI-based) using certified tokens/HSM-backed keys; the system validates the certificate chain and preserves signature validation metadata.

١.٢٤. **Contact Center & CRM Module:**

Provide case management (complaints, disputes, appeals), a ٣٦٠° UTF view, canned responses, and integration with IVR/chatbot. Expose APIs for omnichannel updates.

١.٢٥. **Payments Module:**

A robust payment processing component to handle all fees, taxes, and payments for services. This shall integrate with the Ministry of Finance (MoF) systems and/or approved payment gateways. Key capabilities:

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

١.٢٥.١. Support for online payments (credit/debit cards) through a payment gateway, including multi-channel payments (web portal, mobile app, point-of-sale at offices, kiosks).

١.٢٥.٢. Ability to split payments into multiple accounts automatically. For example, part of a fee goes to the government treasury (state fees/taxes) and another part to the Authority or service provider (service fees). The split shall be configurable for each transaction type and adjustable via administrative settings in case fee structures change.

١.٢٥.٣. Support for an e-wallet or prepaid account mechanism: Users (citizens or stakeholders) could load credit into an account within the system and use it to pay for services, with proper reconciliation to bank accounts. This can expedite frequent transactions and allow the implementer (or Authority) to manage settlements to relevant parties (e.g. inspection center fees, etc.) on a periodic basis.

١.٢٥.٤. Integration with current MoF or third-party e-payment services to report and update payment status in real-time. All payment transactions must be logged with receipts issued to users. The system shall also handle refunds or reversals if needed (with proper authorization).

١.٢٥.٥. See 'Payment Orders & Automatic Flags' below for end-to-end behavior at MoF cashier counters.

١.٢٥.٦. Security and compliance with banking standards Payment gateway and any in-scope components shall provide PCI-DSS v٤.٠ AOC prior to go-live and annually. PCI-DSS Scope & Data Flow. PCI-DSS compliance is scoped to the payment service providers, POS devices, and any third-party components that store, process, or transmit cardholder data. Authority systems shall not store, process, or transmit PAN, SAD, or full track data. Web and mobile flows shall use hosted payment pages / redirect / iFrame / tokenization so that card data bypasses Authority infrastructure. If any Authority-hosted touchpoint is unavoidably in scope, the Bidder shall identify it explicitly and provide the corresponding PCI AOC and segmentation evidence.

١.٢٥.٧. E-Invoicing: Issue tax invoices/receipts with digital signature and QR. Preserve originals and signature validation metadata per retention policy.

١.٢٥.٨. Annual Tariff Tables: Maintain configurable annual fee/tariff tables (effective-dated) that auto-roll on January ١ in line with decreed schedules; support proration and back-dated adjustments with full audit. Amnesty Windows. Configure fee/penalty amnesty periods with start/end dates, eligibility rules, and reporting of foregone amounts.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

١.٢٥.٩. Multi-channel collections (online + physical). The solution shall support payments via: (i) online cards/payment gateway; (ii)bank branch over-the-counter (EBPP/payment code); (iii)Ministry of Finance cashier counters ("Sanādiqal-Māliyyeh"); (iv) licensed money transfer companies; and (v) POS at Authority branches/private centers.

١.٢٥.١٠. Third-Party Service SLAs & Fallbacks:

- External dependencies (payment gateways, banks/EBPP, licensed money transfer, SMS/email, insurance, inspection, customs, DGGS) shall have documented technical and commercial SLAs. The platform shall implement circuit breakers, bulkheads, and retry back-offs per integration, with user-facing fallbacks (queued transactions, vouchers/payment orders) during outages. The Contractor shall monitor upstream SLAs and provide monthly availability and error-rate reports.
- Licensed money-transfer companies shall include, at a minimum, operators such as OMT and Wish (or their lawful successors), subject to Ministry of Finance approval and reconciliation interfaces.

  Each channel must return real-time (or near real-time) payment confirmations and reconciliation records with unique transaction references.

١.٢٥.١١. Payment Orders & Automatic Flags. Support issuance of payment orders linked to Ministry of Finance cashier counters (Sanadiq-al-Māliyyeh). Upon payment status change, automatically apply or lift service/vehicle flags (e.g. holds, renewal blocks) in real time with audit.

١.٢٥.١٢. Third-party fee configuration & settlement. From Back-Office, authorized admins shall configure per-service third-party fees (e.g. Notary fees, Medical Commission, inspection centers, couriers, Sticker issuance/replacement fees…), including VAT/tax flags, effective dates, and split rules. The system must auto-split and settle proceeds by beneficiary on configurable cycles (daily/weekly/monthly) with statements and exportable remittance files.

١.٢٥.١٣. Card Physical Print applied only when the citizen requests a physical card during renewal/replacement When annual renewal activated.

١.٢٥.١٤. Plate and e-sticker fees are modeled as configurable lines. The system auto-splits and settles , on configurable cycles (daily/weekly/monthly), with statement PDFs, CSV remittance files, and reconciliation (paid vs. produced vs. issued).

١.٢٥.١٥. Compliance. Apply KYC/AML/CFT checks appropriate to payment channel; maintain auditable trails of payer identity, channel, and settlement.

١.٢٦. **Data Analytics and Reporting Module:**

١.٢٦.١. Analytics & Reports:

- A business intelligence component to generate reports and statistics on all aspects of the system. The Authority shall be able to get real-time dashboards (e.g. number of registrations per period, revenue collection, number of active vehicles by type, exam pass rates, etc.) and detailed reports for auditing and decision-making. This module shall also allow custom query building and data export for authorized users. It is important for monitoring the performance of decentralized centers (e.g. inspection centers activities, notary transaction counts, etc.) and tracking any irregularities (possibly feeding into an audit log analysis for security).

١.٢٦.٢. Data Quality & Analytics Service Levels:

- The MDM/dedup engine shall achieve Authority-approved precision/recall targets for person/vehicle matching, reported on nightly DQ scorecards with trendlines and remediation queues. Canned dashboards must load in ≤ ٥s P٩٥ for defined filters; ad-hoc queries run in governed workspaces with workload isolation. Materialized UTN-centric views are refreshed per SLA and include data-freshness indicators.
- UTN Data Umbrella & ٣٦٠°. All subject area marts (Vehicles, Licenses, Violations, Payments, Appointments, External Checks) shall key on UTN, enabling one-click ٣٦٠° views and cross-agency queries (police, customs, insurance) via the integration hub. Provide UTN-centric materialized views and indexes for high-volume lookups (≤ P٩٥ ٢.٠s at peak) and canned ٣٦٠° reports.
- MDM & Data Quality. Maintain golden records for Persons, Vehicles, Centers, Dealers with survivorship rules, periodic dedupe runs, and data quality dashboards.
- Safety Analytics. Deliver GIS crash hot-spots, violations heatmaps, inspection failure patterns, and a KPI pack (first-time pass, wait time, renewal cycle time, fraud flags).

١.٢٦.٣. Prebuilt Reports:

Provide out-of-the-box, exportable reports:

- Registrations within a selectable period;
- User activity (login/logout with timestamps and session metadata);
- Registration productivity statistics (average handling time per user/device; daily/weekly counts); and
- Additional configurable templates as defined by the Authority.

١.٢٦.٤. Instructor/Examiner Productivity & Remuneration Reports:

Provide locked, audit-ready aggregates and exports (CSV/PDF) for remuneration and

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

billing: per instructor/examiner candidate counts, pass rates, scheduled vs. completed tests, billable minutes/sessions by center, and exception lists (spoiled/corrected results with maker–checker IDs). Figures used for payment are versioned and reproducible from source logs.

١.٢٧. E–Sticker Module (Optional)

١.٢٧.١. Policy Optionality & Activation Reference.E–Sticker optionality, activation/deactivation, feature–flag control, and graceful–degradation requirements are governed by §١.٢٨.٢ (canonical).

١.٢٧.٢. Readiness While Disabled. The SI shall submit an import/logistics plan and pricing as part of the offer. No sticker procurement, shipment, permitting, warehousing, commissioning, or payments shall occur until the Authority issues a written Activation Notice as defined in §١.٢٨.٢.

١.٢٧.٣. Commercial Standstill. No payments for sticker goods or sticker–specific services are due, and no financial run–rates shall accrue, unless and until an Activation Notice is issued by the Authority per §١.٢٨.٢.

١.٢٧.٤. Operational Scope While Disabled. While the e–sticker feature flag is disabled, the Contractor shall maintain background readiness only: master data and UID ranges, inventory controls, interface availability (APIs/portals), and acceptance testing in SEC/UAT. No field issuance, no production encoding, and no contractor run–rates shall occur until activation per §١.٢٨.٢.

In summary, all in–scope manual or semi–automated processes shall be discovered and mapped, then validated and normalized into TO–BE BPMN ٢.٠ process models and DMN ١.x decision models and incorporated into the platform; these models become the authoritative build artifacts and are maintained in the RTM. Bidders are expected to analyze existing workflows, streamline them, remove redundancies, and introduce digital verification where applicable. The end goal is a fully digital service delivery model where citizens and stakeholders can complete most tasks online (except where law requires in–person steps), and internal efficiency is greatly improved through integration and automation.

١.٢٧.٥. Requirements for Electronic Vehicle Stickers (E–Stickers).

١.٢٧.٦. Sticker media and RFID–capable encoding/printing hardware are in scope and shall be supplied, installed, and supported by the SI. The SI shall design, host, and operate all digital capabilities for e–stickers—policy toggles, issuance orchestration, UID management,

encoding orders, anti-tamper validation, inventory, lifecycle (issue/replace/deactivate), roadside verification APIs, and analytics—regardless of whether stickers are activated on day one. Graceful-degradation and non-dependency behavior shall follow §١.٢٨.٢.

- Sticker Purpose and Function: The sticker will serve as an easily checkable proof that a vehicle is properly registered and that it has passed inspection and is insured. The sticker effectively links the physical vehicle to the digital record in the system in real-time.
- Policy Optionality & Alternatives: Implementation of RFID e-Stickers is optional and may be phased. The Authority may cancel the sticker requirement owing to ecosystem. The platform shall support either policy without impacting other services.
- Technology: The stickers shall use RFID (Radio Frequency Identification) technology for automatic identification. Specifically, passive UHF RFID tags are commonly used for vehicle identification because they can be read from several meters away by roadside readers or handheld devices. Key specs:

  The RFID tag embedded in the sticker must ensure compatibility with standard readers. It shall have a unique identifier that, when read, corresponds to the vehicle's record in the database. For security, the data on the tag can be a random unique number (no meaningful data, just an ID) so that if someone scans it, they can't glean info without access to the database. The system would then retrieve all needed info when it sees the ID.
- Usage Scenarios of Stickers (if implemented): The e-sticker will enable various improvements:
  - Roadside Checks: Police cars equipped with UHF readers could drive by and automatically scan the tags of nearby vehicles, instantly flagging any vehicle that is unregistered, expired, reported stolen, or on a watchlist, without having to stop each one. This greatly improves enforcement efficiency.
  - Entry/Exit Points: Readers at border crossings or ports can scan vehicles to quickly check their status.
  - Parking or Toll Integration: In the future, the same sticker could be used to integrate with parking systems or toll systems (though toll would likely use separate tags if needed, but a unified approach is possible if planned).
- Yearly Renewal Indication: it could be used as a quick visual cue of valid inspection year.
- Replacement and Management:

- When a vehicle is newly registered, a sticker is issued and linked to it. If the vehicle changes owner but remains registered, typically the same sticker can remain (unless the number or any key info changes).
- If registration lapses or vehicle is scrapped, that sticker ID is voided in the system.
- If a sticker is damaged or windshield replaced, the owner will need a replacement sticker. The system must allow issuing a new sticker and invalidating the old one (ensuring the old ID is marked not to be accepted if read).
- The system shall track sticker serials/IDs: which ones are issued, which are in stock, and ensure one-to-one with vehicles.
- providing an initial supply of these RFID stickers and the necessary equipment to encode them if needed and requested.

Exclusion Clause: Phased Implementation. E-sticker rollout may be phased or deferred at the Authority's discretion. The platform must fully support activation/deactivation without impacting other services or data integrity. The platform SHALL operate fully with or without e-stickers; if deactivated, all dependent flows must degrade gracefully.

In summary, the electronic vehicle sticker will be a modern way to link physical vehicles to digital records. It leverages RFID technology for quick, mass-scale verification. Implementing it will require careful attention to security and process (to avoid misuse), but it stands to greatly improve compliance monitoring when fully utilized.

١.٢٧.٧. Requirements for the Electronic Sticker Issuance System

- Issuance & Orchestration (In-Scope Supply). Sticker rolls/inlays and RFID-capable printers/encoders shall be supplied under this RFP by the SI, who will also operate the Issuance Orchestrator to: (i) allocates UIDs/EPCs, (ii) creates encoding work-orders, (iii) validates post-encode read-backs, (iv) records spoilage/reprints, (v) associates the encoded tag to the Vehicle ID and registration event, and (vi) controls replacement flows (windshield change/damage) with deactivation of prior tags.
- Sticker Encoding Devices: The hardware needed to program (encode) the RFID stickers with the correct data. This could be:
  A dedicated RFID encoder device or printer. Some label printers can encode UHF RFID in lays and also print on the sticker at the same time. Alternatively, a separate desktop encoder pad could be used if no printing is required.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

If the sticker is pre-printed and only needs encoding, an encoder pad where you place the sticker to program it might suffice. But it might be efficient to print at least a minimal detail (like plate number or expiry year) on the sticker, so a printer with RFID capability might be ideal.

The vendor shall specify the model and type of encoder/printer and ensure it's calibrated for the specific sticker tags provided.

- Integration with Registration Process: When a new vehicle registration or renewal is processed, the system shall prompt for sticker issuance:
  - For a new registration: after plate number assignment and entry of all data, the system shall provide the next available sticker ID to encode. The operator will run the encoding step, which writes the vehicle's unique code to the tag and prints any necessary text on it. The system then associates that sticker's ID (and serial number if any) with the vehicle record.
  - For renewal: if the policy is to issue a new sticker each year, then upon renewal, a new sticker is encoded and the old one is instructed to be removed (the owner shall remove the expired sticker and replace with a new one)
  - For transfer of ownership: Typically, the sticker can remain since it's tied to the vehicle, not the owner. But the system might decide to issue a fresh sticker whenever new plates are issued (if plate number changes). If number stays same, no need for a new sticker, just update owner info in back-end.
- Issuance Locations. Enable sticker encoding/printing at branch offices and designated installation centers, with per-site inventory tracking and issuance logs.
- Sticker Inventory Management: Just like cards, the blank stickers (with embedded RFID) shall be tracked:
  - Stickers may come in rolls or sheets; each has an identifier (RFID has a unique code which can be read even before programming, plus often a human-readable serial printed by manufacturer).
  - The system shall log which sticker IDs have been used (and on which vehicle) and which are still available. This prevents, for example, someone taking a sticker from stock and using it outside the system.
  - If a sticker is spoiled (encoded incorrectly or printing smudged), it shall be recorded as void and a new one used.
  - Branches/centers shall have a supply count, with thresholds for reordering new stock.

- Reading and Verification Equipment:
  - While issuing, it's important to verify the sticker's functionality:
  - The encoder/printer shall double-check by reading the tag after encoding to ensure the data was written correctly.
  - Also, hand held RFID readers shall be provided to test stickers and for use by staff or law enforcement These could be integrated with a mobile app for law enforcement.
  - The system shall allow authorized users to input a sticker ID and retrieve which vehicle it belongs to (for troubleshooting or enforcement queries).
- Issuance and Attachment Process: The system needs to define how stickers get to vehicles:
  - If issuing at branch: after encoding, the sticker is handed to the vehicle owner with instructions to affix on the windshield (and perhaps a diagram on where exactly). The system shall mark that sticker as "issued" to that person.
  - If a vehicle is being registered at a decentralized center, possibly that center will have the encoding equipment as well. If in future, they might need a small encoder to issue the sticker on site when they hand over a new car to a buyer.
- Lost/Damaged Sticker Replacement: The system must handle cases where an owner needs a new sticker because the old one got damaged (windshield replaced, etc.):
  - Verify the old one is deactivated (to avoid duplicates).
  - Issue a new one and possibly charge a replacement fee if policy dictates. The system shall incorporate that fee handling in the payment module.
  - Ensure at any time only one active sticker per vehicle.
- Scalability: If, for example, ٢-٣ million vehicles will use stickers, the system must handle that volume in its database and issuance process. The encoding shall be fast (UHF encoding typically is quick, under a second each) and printers can handle at least dozens per minute if needed. Bidders shall ensure the equipment can manage any batch operations.
- Dual-control & maker-checker: Encoding job release and post-encode activation require two distinct users; audit log records user IDs, device IDs, and signed hash of payload.
- Read-back cryptographic check: Post-encode, the reader computes HMAC-SHA-٢٥٦(EPC||TID||Vehicle ID) and compares to the work-order token; mismatch ⇒ auto-spoil + rework.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

- Stock governance: Per-site cycle counts weekly; variance > ٠.٥٪ triggers investigation report.

The sticker issuance system will bridge the gap between digital system and physical vehicle presence on roads. By providing the encoding tools and ensuring every active vehicle is tagged, it sets the foundation for a smarter traffic management and enforcement ecosystem. The vendor's proposal shall clearly detail the model of sticker used, the encoder/printer devices, and how they will implement this process efficiently across all centers.

١.٢٨. Secure License Plate Management Module

License Plates – Separate Procurement.

١.٢٨.١. The Authority will procure license plates under a separate RFP. The Selected Integrator (SI) shall own the end-to-end digital lifecycle, control, and orchestration for plates (by integration) including:

- Master data, serialization ranges, and anti-duplication controls for plates.
- Work-order creation, fulfillment status, QA/acceptance, spoilage/reprint handling, and chain-of-custody logs (who/when/where) for issuance, replacement, return, and destruction.
- Inventory at all nodes (central, branches, contractors, couriers) with lot/roll tracking, and threshold alerts.
- Appointment/installation scheduling, handover capture, and proof-of-delivery (photos, signatures, GPS/time).
- Fee calculation and third-party settlement (plates) via the Payments Module, with configurable splits and remittance statements to the respective contractors.
- Open, secure APIs/portals for the Plate Contractor plus a sandbox for Authority-approved integrators (e.g., law enforcement, couriers).
- Full auditability (immutable logs), dashboards, and SLA monitoring.

١.٢٨.٢. Policy Optionality – E-Sticker Feature Flag (Canonical). The e-sticker program is optional and may be phased, deferred, or canceled at the Authority's discretion. The platform must operate fully with or without e-stickers. A feature flag SHALL control all e-sticker functionality; activation or deactivation must be possible without code changes. All dependent flows must degrade gracefully (no hard dependency on stickers). Verification endpoints SHALL accept plate number, VIN, QR token.

Verification endpoints shall accept plate number, VIN, QR token, or (when enabled)

EPC/plate-RFID uniformly via a single API, allowing feature flags to add/remove modalities without breaking integrators.

In summary, the system must provide a full lifecycle solution for vehicle and driver management – covering front-end services to citizens and stakeholders, as well as back-end processing by the Authority's staff – all within one unified platform. The vendor is expected to deliver all required software applications for the above components, configure them to meet Lebanese laws and procedures, and ensure all existing functionalities of the current system are replicated (unless otherwise decided to be dropped) and improved upon with these new features.

١.٢٨.٣. Requirements for Secure License Plates

Secure plate blanks, reflective sheeting, embossing, hot-stamp foils, and production machinery will be supplied and operated by a separate plate contractor under a separate RFP. The SI is responsible for the digital control plane: plate series definition, order orchestration, QA acceptance, inventory/lot tracking, handover to citizens, returns/destruction, and end-to-end auditability.

Plate Number Management: The system will maintain an inventory of all plate numbers issued (and those available for issuance). For secure plates:

- The numbering format and the range of numbers for each category shall be defined by the Authority. current numbers remain, and new series would continue from where old left off, or redefined if needed .
- Expired or Replaced Plates: If a vehicle is deregistered or plates are replaced (e.g. format change or damaged plate), the system shall mark the old plates as invalid. physically, old plates will be collected and destroyed to prevent misuse.

١.٢٨.٤. Requirements for the Secure License Plate Issuance System

Plate manufacturing is executed by a separate contractor. The SI shall provide the Plate Order Management module that generates machine-readable jobs (text/layout/type), receives production and QA status, books inventory movements, and controls chain-of-custody through to citizen handover (including proof-of-issuance and old-plate collection/destruction). Only jobs created by the core system may be produced (no free-text production). Support 'Diplomatic' and 'Consular' vehicle categories with unique plate series, exemptions, and approval workflows.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

The Plate Contractor operates Authority/SI-provided tools only; no software development or hosting is required from the Plate Contractor.

- Plate Personalization Software (Provided by SI): The SI shall supply, install, and support the software and/or edge agent that (i) receives machine-readable jobs from the core system, (ii) drives approved embossing/printing equipment, and (iii) posts back status/QA and chain-of-custody events. The Authority operates this SI-provided software; no development by the Plate Contractor is required:
  - It shall maintain a queue of plate orders, each specifying the text/number to emboss and the plate type.
  - each site's system will handle its own requests, and connected to the central database to mark plate produced.
  - The software shall also handle reorders (if a plate was misprinted or if a duplicate is needed).
  - Integration: the main system, upon completion of a vehicle registration that needs new plates (e.g. new registration or a number change), will trigger the plate order automatically. Conversely, the plate system shall confirm back once the plate is made.
- Quality Control:
  - The plate issuance process must ensure each plate produced is correct
  - Visual checks by the operator for embossing errors or defects in the plate.
  - If using automated systems, sensors or cameras might verify the embossed text against the order.
  - Any plate that is not up to standard shall be discarded (and the system inventory adjusted to allow a remake).
  - The system shall track blank plate usage. For example, each produced plate uses one blank; the blank's ID can be associated with the plate number for traceability. The inventory module shall alert when blanks are low so more can be ordered.
- Distribution of Plates:
  - the citizen can get them immediately on site, which is a plus for service speed.
  - the chain of custody must be secure so plates don't get lost or swapped. Logging which employee handed the plate to the owner is part of accountability.
- System Security and Audit: Because license plates are a controlled item (they give Authority to operate a vehicle):

- Only authorized staff shall be able to trigger production of a plate. The system shall log who requested and who produced each plate.
- There shall be measures to ensure no unauthorized plate numbers are made. The production system shall only accept jobs from the official software .
- Completed plate jobs shall mark the plate as active on a vehicle in the database. If someone tries to request a plate number that's not in the system (e.g. a fake request), it shall be caught.

- Authorized Plate Embossing Shops:
  - Authorized embossing shops. The solution shall support licensing and governance of authorized plate embossing shops: onboarding, user roles, secure blank inventory, job orders from the core system only, production logs (who/when/machine), periodic audits, and reconciliation of blanks vs. produced plates. Shops operate using approved equipment and consumables; the system enforces serial/lot tracking and spoilage recording with photographic evidence.
  - The license plate issuance system is the physical manufacturing wing of the registration process. It must be tightly integrated with the digital system and maintain high security and accuracy.

٨. BACK-OFFICE ADMINISTRATIVE FUNCTIONS

١.٢٩. Digital Staff & Affiliate Virtual ID Cards: Provide a module to issue and manage virtual ID cards for Authority staff and affiliated personnel (examiners, driving-school owners/instructors, operators). Cards appear in the mobile app and portals, bound to the user's UTN and device, and show only necessary data (name, role, card ID, status, expiry). Each card carries a PKI-signed QR for offline/online verification, with no PII in the QR payload. Include maker-checker approval for issuance/suspension/revocation, lifecycle states (Active/Suspended/Revoked/Expired), and audit logs for all actions and scans. Support notifications for issuance and pre-expiry.

١.٣٠. User Management and Permissions:

An admin interface to manage system users (Authority employees, branch users, inspectors, etc.) with role-based access control. Different roles will have access only to the functions they need. For example, an inspector might only record inspection results, a cashier role might only handle payment confirmations, a supervisor can approve certain transactions, etc.

١.٣١. Enterprise Identity & Access Integration:

Staff-facing systems shall support SSO via SAML ٢.٠ and/or OpenID Connect (OIDC) against the Authority's IdP, with both IdP-initiated and SP-initiated flows. Citizen and stakeholder portals shall use OIDC with optional federation to national e-ID as available. Implement SCIM ٢.٠ for automated user lifecycle (provision, update, deprovision) and role mapping from HR/ERP sources. Step-up authentication policies (MFA) shall be configurable per action/risk, with transaction signing where required. All access decisions must be logged with subject, client, and device context.

١.٣٢. Customer & Entity Change Management:

Provide verified change-of-name and address workflows for persons and companies with document capture and downstream propagation (licenses, registrations, permits).

١.٣٣. Bulk Fleet Actions & Corporate Events:

Enable bulk renewals, exports, number` changes, and ownership transfers via CSV/API for fleets. Support mergers/acquisitions with mass reassignment of vehicles and permits from absorbed entities with full audit.

١.٣٤. System Configuration:

The system shall provide configuration screens for administrators to update reference data without vendor intervention – e.g. fee amounts for each service, list of vehicle makes/models , inspection criteria, fine categories and amounts (if changed by law), points thresholds, etc. Much of the business logic shall be data-driven and configurable to adapt to regulatory changes quickly.

١.٣٥. Feature Flag – Annual Card Renewal:

Provide registrationCard annualRenewal , effectiveFrom and maker-checker approval. All changes audited; no code changes required.

١.٣٦. Audit Trail and Monitoring:

Every transaction (creation, update, deletion of records; approvals; logins; etc.) must be logged with user ID, timestamp, and details. There shall be an audit module for internal auditors or managers to review these logs. Additionally, any sensitive changes (like waiving a fee, voiding a fine, altering an owner name outside a transfer process) shall require a higher-level authorization and be clearly tracked. For transactions requiring authorization, the system shall initiate a workflow in which the direct supervisor or the authority president reviews and approves the transaction digitally, ensuring a fully automated process.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

١.٣٧. Operational Monitoring & Incident Management:

Define severity levels and targets: P١ (critical service outage) MTTD ≤ ٥ min, MTTR ≤ ٢ h; P٢ MTTR ≤ ٨ h. Provide ٢٤×٧ on-call with escalation paths, stakeholder comms templates, and status pages. Security incidents must be notified to the Authority within ٢٤ hours with initial indicators, and a full Root Cause Analysis (RCA) within ٥ business days including corrective/preventive actions. Observability dashboards (APM, logs, metrics, traces) shall be shared with the Authority NOC/SOC.

٩. HYBRID MOBILE APPLICATION

١.٣٨. User Portal and Mobile Application

١.٣٨.١. The system shall include a Citizen Portal (web-based) and a Mobile App for end-users to access services online. Citizens SHALL be able to initiate all formalities and upload all required documents, which triggers a back-office workflow at the Authority. Once the submission is validated (where applicable) the new physical documents (e.g., registration card) are printed and ready, the citizen will visit the Authority once to hand over originals, pay any remaining fees, and receive documents in a single appointment ("one-shot" issuance). Through these channels, users shall also be able to: pay fines, schedule driving tests, check application status, update contact information, and download digital documents. The portal/app shall provide a wizard-based process for complex services with prerequisite checks and digital issuance.

Notifications/reminders (expiry alerts; exam results) are included. Vehicle renewal appears as an optional service, activatable only upon Authority approval

١.٣٨.٢. Citizen choice for physical card: During renewal (when Annual Renewal Mode is active) or at any time for replacement, the portal/app offers an optional "Print physical card" step. If selected, fees are calculated, fulfillment is queued for pickup or courier, and status is tracked. If not selected, digital-only renewal completes with QR/verification.

١.٣٨.٣. When stickers are active, the portal/app displays sticker status (Active/Blocked/Replacement Required) with replacement request flow (windshield change) and appointment/fee handling. When disabled, the UI hides sticker features without exposing errors.

١.٣٨.٤. The mobile app in particular shall allow users to display a digital driving license or vehicle registration card (a QR code or barcode that law enforcement can scan to verify

authenticity). The portal and app must be trilingual (Arabic, English, and French) and user-friendly, reflecting a modern e-government service.

١.٣٨.٥. User Activity Timeline (Portal & Mobile). Provide a chronological activity feed per user (UTN), showing actions and requests across channels (portal, mobile, branch, delegated/courier), with timestamps, status, reference IDs, and deep links to the underlying case/service. The feed must include payments, applications, appointments, deliveries/handovers (with proof-of-delivery thumbnails), approvals/rejections, and document downloads. Support filters (date range, service type, status), keyword search, and export (PDF/CSV). Clearly label the actor ("self", "authorized delegate/courier", or staff role) and capture device/IP and location (where permitted). Respect privacy: citizens see only their own feed; delegates see only consented transactions; retention follows the Records Policy. Push real-time updates to the timeline upon state changes.

١.٣٨.٦. The system shall issue, store, and present digital versions of both the driving license and the vehicle registration card in the mobile app, with offline-verifiable QR/signatures, full parity with the physical credentials, and revocation/rotation controls.

١.٣٨.٧. Mobile App KPIs

- Crash-free sessions ≥ ٩٩.٥٪ monthly; cold start ≤ ٢.٥s on reference mid-tier devices.
- Offline mode for credential verification (QR/signature check) with secure sync on reconnect.
- Root/jailbreak detection, certificate pinning, OS attestation, and secure key storage as mandatory.

١.٣٨.٨. Citizen Document Upload & Pre-Validation (Portal & Mobile)

١.٣٨.٨...١. Per-Service Checklists. For each service, display an Authority-approved, dynamic checklist of required documents (by applicant type, vehicle category, and scenario), with inline examples and templates.

١.٣٨.٨...٢. Capture UX (Web & Mobile). Guided capture with auto-crop, de-skew, glare detection, perspective correction, and background cleanup; support multi-page scanning and merge to PDF.

١.٣٨.٨...٣. Allowed Formats & Limits. Accept PDF, JPEG, PNG. Maximum ٢٥ MB per file and ١٠٠ MB per case by default (configurable per service). Enforce server-side MIME/type sniffing (no extension-only checks).

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

١.٣٨.٨...٤. Resumable/Chunked Upload. Support resumable, chunked uploads with automatic retry and client-side compression for images. Show progress and estimated time remaining. Drafts auto-save for ٧ days (configurable).

١.٣٨.٨...٥. Security & Integrity. Perform AV/malware scanning, content-type validation, and restricted content checks. Strip EXIF/GPS metadata from citizen uploads. Compute SHA-٢٥٦ hashes for each file; retain in audit.

١.٣٨.٨...٦. OCR & Auto-Classification. Apply OCR and document classification to extract key fields (e.g., VIN, plate, ID number, names, dates) and pre-fill forms where possible. Confidence thresholds are visible to reviewers; low-confidence fields are highlighted for manual verification.

١.٣٨.٨...٧. Metadata & DMS Linkage. On successful upload, store document class, subtype, applicant UTN, vehicle UTN, service case ID, and capture timestamps. Push documents and metadata to the Authority DMS with a two-way link per §١.٢ (Digital Archiving & DMS Integration).

١.٣٨.٨...٨. Legibility & Completeness Checks. Validate presence of mandatory pages/signatures/stamps based on the document class. Block submission if required items are missing, and provide targeted error messages.

١.٣٨.٨...٩. e-Signatures & Consent. Where permitted, support qualified e-signature of application forms and consent statements; capture on-device handwritten signatures for non-qualified flows.

١.٣٨.٨...١٠.Originals at One-Shot Visit. For documents that legally require originals, the portal/app shall label them “Original required at visit.” Back-office validation proceeds on scans; final issuance occurs only after originals are verified during the one-shot appointment.

١.٣٨.٨...١١.Notifications & SLA Timers. Upon submission, create a workflow task with SLA clocks; notify the citizen on acceptance/rejection or requests for re-upload. All events appear in the §١.٣٨.٥ Activity Timeline.

١.٣٨.٨...١٢.Accessibility & Languages. All upload and guidance flows are Arabic/English/French and WCAG ٢.٢ AA compliant.

١.٣٨.٨...١٣.Privacy & Retention. Apply data minimization, masking, and retention per §١٥ (Legal & Regulatory) and the Records Retention Schedule; enforce role-based viewing/downloading and watermarking for staff previews.

١.٣٨.٨...١٤.KPIs & Quality. Upload success rate ≥ ٩٩.٧٪ monthly; average time-to-first validation decision ≤ ٢ business days (configurable by service); OCR auto-classification accuracy ≥ ٩٥٪ on approved samples prior to go-live.

١.٣٩. External Stakeholders Portal:

Besides notaries, other stakeholders require access:

١.٣٩.١. Driving Schools:

A portal for driving schools to register their students for driving tests, submit required documents, and schedule exam appointments. Driving schools shall be able to view exam results for their candidates and possibly receive certifications digitally. Provide a full school portal/API for candidate management, scheduling, result retrieval and billing models: (i)per-transaction fees; or (ii)annual subscription with usage caps/overage. Support wallets/prepaid balances, invoices, and SLA dashboards. Issue digital accreditation/permit cards for licensed driving schools and for individual instructors, viewable in their portal and as QR-verifiable credentials in the mobile app. Each digital card shall display license/permit number, validity, categories, and authorized centers; expirations drive automated reminders and issuance hard-stops per policy.

١.٣٩.٢. Medical Commission / Physicians:

Medical fitness certificates are required for license categories or renewals, thus, an interface for authorized doctors to update the system on an applicant's medical fitness should be provided (a role on the web portal for physicians shall be present to cover this flow).

- Remote Liveness Capture. The physician portal SHALL use the device camera (laptop webcam preferred) to capture a short liveness check during certification and compute a confidence score. The liveness decision and score(s) are stored with the applicant's UTN for later review.
- Acceptance Baseline. Prior to go-live, the Authority sets the minimum acceptable liveness thresholds during UAT (baseline pass/fail and score threshold). These thresholds are configurable and enforced at runtime; submissions below threshold are rejected or routed to in-person review.

١.٣٩.٣. Customs/Ports:

There is a need to integrate with customs systems to receive customs-certificate (شهادة جمركية) information for imported vehicles

١.٣٩.٤. Dealerships:

The system may support dealership accounts to pre-register new vehicles and process registrations, subject to approval by the Authority.

١.٣٩.٥. Law Enforcement Access:

A secure interface (or web services) for Internal Security Forces (police) to query vehicle and driver information using plate number, license number or national ID. This interface shall provide needed details (validity of registration, license status, outstanding violations, etc.) and allow for roadside actions such as marking a license as confiscated/suspended or verifying a digital license/sticker authenticity.

١.٣٩.٦. Security agencies & judicial checks:

Where permitted by law, integrate with the General Directorate of General Security (DGGS) for foreign nationals' entry/residency status validation, and with Ministry of Justice/Police services for judicial records/watchlists to enforce service hard-stops (e.g. travel bans, court holds). Apply strict data minimization and audit. When e-stickers are enabled, roadside apps can read EPC/QR and resolve vehicle status via offline signature or online query. If stickers are disabled, the same app flows remain available using plate/VIN queries. The roadside app shall verify sticker authenticity using:

- UHF EPC (if enabled);
- QR with offline signature, or
- plate/VIN. The app works offline using a daily CRL/allow-list snapshot and local signature keys; sync on reconnect.

١.٣٩.٧. UTN-centric Queries. Roadside and back-office tools shall query by UTN, plate, VIN, or license #, with results anchored on UTN for consistency across violations, holds, impounds, and credentials.

١.٣٩.٨. Postal/Courier Providers. Integrate with licensed private couriers for pickup/delivery of cards, stickers, and plates: create consignments, print labels, track milestones, capture proof-of-delivery, and reconcile COD (if applicable).

Create consignments and labels for cards, stickers, and plates; track milestones and capture proof-of-delivery. Chain-of-custody entries must bind item serials (card/plate/sticker) to the consignment.

Authorize licensed couriers as Delegated Service Agents to initiate and complete permitted workflows on behalf of citizens with explicit consent. The module shall capture and bind consent to each transaction, enforce role-scoped permissions (no access beyond the task),

and record full audit logs (who/when/where/device). Couriers operate via a secure portal/app with KYC onboarding, data minimization, and chain-of-custody continuity from pickup through delivery.

١.٣٩.٩. **Sectoral Authorities:**

Provide role-scoped portal/API access for designated authorities (e.g., Rokhas Nakel, MoI, MoA, others added by configuration) to publish, suspend, or revoke permit status; expose read-only status to Authority staff and law enforcement; all actions are audit-logged and drive automatic gating per §١.١٢.١٤.

Security controls for the mobile app and digital credentials are defined separately under Technical & Security Requirements – Mobile App & Digital Credential Security.

١٠. DECENTRALIZED SERVICE CENTER OPERATIONS

As part of modernization, services that are currently centralized shall be accessible from multiple decentralized centers:

١.٤٠. The system must support operations in all existing regional branch offices (~٧ branches currently) and any future authorized private centers (for inspections or even certain registration services). Each center or branch will have appropriate access to the system with role-based permissions.

١.٤١. Extended Hours Support: The system shall be available beyond traditional working hours (potentially ٢٤/٧). This implies robust uptime and possibly different user roles performing data entry during off hours. It shall log transactions by center and user for accountability.

١.٤٢. The system must ensure data consistency if multiple centers are operating concurrently on the same processes. For instance, if a vehicle renewal can be done at any center, once processed at one location, it shall immediately reflect in the central database to prevent duplicate processing.

١.٤٣. Expansion Centers: The solution shall support additional service to improve throughput and service times; all workflows, licenses, and capacity plans must scale accordingly.

١.٤٤. Deployment Flexibility: The Contractor shall implement the system, updates, and modifications at any locations designated by the Authority (headquarters, regional branches, and future centers) with the same security and operational standards.

١.٤٥. Portal and Self-Service: Most services shall be available online for self-service by citizens, reducing the need to visit offices.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

١.٤٦. End-to-End Online by Default: All citizen- and stakeholder-facing services must be deliverable fully online (application, document upload, scheduling, payments, approvals, and digital credential issuance) without mandatory in-person steps except where explicitly required by law or for physical actions (e.g. biometric capture, practical road tests, or handover of plates/stickers/cards). Physical branches operate as optional fallbacks; online flows remain authoritative.

١.٤٧. Driving License services online: applications for renewal or replacement shall be doable via the portal/app with digital uploads of any required documents and online payment. For new license issuance, the theory test could be computerized, and results fed into the system; practical test scheduling can be done online, though the test itself is in person.

١.٤٨. Vehicle services online: as noted, renewals and even initiating transfer of ownership (with integration to notary for finalization) could start online. The system shall allow a seller to initiate a sale by inputting buyer info, then notify the notary to complete the legal step, and finally let the buyer pay fees online to complete the transfer, coming only to collect new plates if needed.

١.٤٩. Appointment Booking: The system shall allow citizens to book appointments for any in-person service (e.g. vehicle inspection, driving test, or visiting a service center if necessary to pick up physical items or for services that still require presence). This reduces crowding and improves service efficiency.

١.٥٠. Queueing & Capacity. Integrate with token/queue systems, display real-time wait times, and run SLA timers per step. Apply capacity rules per center and auto-throttle appointment availability.

١١. MAINTAINABILITY AND DOCUMENTATION

The solution shall be maintainable by the Authority in the long run. This means:

١.٥١. The codebase (for custom-developed components) shall follow clean coding practices and be well-documented. The vendor must supply source code escrow or deliver source code to the Authority (as soon as any module go into production) for future in-house maintenance.

١.٥٢. Configuration documentation and system administration manuals must be provided so that Level ١ support staff at Authority can handle routine issues.

١.٥٣. The design shall aim to minimize the need for constant vendor intervention for changes. For example, adding a new type of fee or a new service in the workflow shall be achievable

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

through configuration (in the Backoffice) or minor customization rather than a major code rewrite.

١.٥٤. The vendor shall propose a knowledge transfer plan and training programs to equip Authority's IT personnel to eventually manage basic support, with the vendor focusing on higher-level support (as per maintenance levels L٢–L٤).

١٢. MANDATORY DELIVERABLES

١.٥٥. Process Discovery & Documentation (Base Scope). Using the Authority Handover Package and stakeholder sessions, the SI shall validate AS-IS, resolve conflicts, and deliver TO-BE BPMN ٢.٠ process models and DMN ١.x decision models for all in-scope services within ٨–١٢ weeks of NTP. Models must become the authoritative build artifacts and be maintained in the RTM.

١.٥٦. HLD/LLD, data model ERDs, interface control documents, and versioned API specs.

١.٥٦.١. For license plates, deliverables include the Portal user guide and SI-provided edge agent/driver documentation. No API deliverable or development is required from the Plate Contractor.

١.٥٧. Migration strategy, rehearsal scripts, cutover/rollback plan.

١.٥٨. Operations runbooks (NOC/SOC), DR runbook, backup & restore playbooks.

١.٥٩. As-built diagrams (network, infra, apps), capacity model.

١.٦٠. SBOMs, SCA reports, vulnerability management plan.

١.٦١. Training plans/materials for L١ and business users.

١.٦٢. End-user/operator training for front-office clerks, branch users, inspection centers, exam committees and notary users on the provided applications (including hands-on labs). Include train-the-trainer, minimum class counts per site, and post-go-live floor-walking support.

١.٦٣. Requirements Traceability Matrix mapping every "shall" to a verification test and artefact.

١.٦٤. Source code delivery/escrow and licensing bill of materials.

١٣. INTELLECTUAL PROPERTY & LICENSING

The Authority receives perpetual, royalty-free usage rights for all deliverables deployed on-prem, including source code for custom components delivered at first production use. Third-party licenses (by core/CPU/user) shall be enumerated with versions and renewal terms. No component may require vendor cloud connectivity ("call-home") for runtime. Source code escrow triggers include vendor insolvency or material breach; build pipelines and SBOMs are deposited at each major release.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

١.٦٥. Software License Term, Renewal & Co-Termination

١.٦٥.١. Lifetime/Perpetual First, Mandatory if Available.

Where an OEM/publisher offers lifetime or perpetual licenses, the Bidder shall supply such licenses (perpetual usage rights) and include software assurance/updates & vendor support entitlements through Year ٦ (twelve (١٢) months beyond the SI's ٥-year maintenance commitment). Perpetual licenses must be registered to the Authority and remain valid without any vendor cloud "call-home" requirements.

١.٦٥.٢. If Lifetime/Perpetual Not Offered — Take the Longest Term + Pre-Fund Renewals.

Where lifetime/perpetual is not offered, the Bidder shall procure the longest available term (e.g. ٥-year, ٣-year, etc.) and pre-purchase/contractually secure all successive renewals to ensure uninterrupted license entitlements, updates, and support through Year ٦. All renewal costs must be included.

١.٦٥.٣. Minimum Coverage Rule (١-Year SKUs).

If the shortest SKU is ١ year, the Bidder shall provide six (٦) consecutive years of coverage (co-termed) starting at Production Go-Live Acceptance, such that all licenses remain fully active for the entire sixth year following Go-Live.

١.٦٥.٤. Co-Termination & Timing.

All license terms and support entitlements shall be co-termed and renewed no later than ٦٠ days prior to each expiry, with proof of renewal delivered to the Authority. Entitlements must remain continuous with no lapse.

١.٦٥.٥. Account Ownership & Transfer.

All licenses/subscriptions shall be registered to the Authority from day one (not to the SI or a reseller). The SI shall hand over tenant/org admin rights, license keys, entitlement IDs, and publisher portal access upon Go-Live and keep them updated throughout the term.

١.٦٥.٦. No Lock-In / On-Premises Independence.

No licensed component may require ongoing vendor cloud connectivity for runtime. Telemetry/activation, if unavoidable, shall be locally proxied and must not degrade or disable functionality if external connectivity is unavailable.

١.٦٥.٧. Remedy for Lapse.

Any lapse in entitlements is a material breach. The SI shall, at its own cost, immediately reinstate coverage (including back-dated support rights) and provide service credits per SLA.

١.٦٥.٨. Evidence & Audit.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

The SI shall provide a Licensing Bill of Materials (LBOM) listing SKUs, quantities, terms, renewal dates, and Years-١-to-٦ coverage mapping, plus annual publisher confirmations of entitlement. The LBOM is maintained in the RTM and updated at each release.

Definitions: "Year ٦" means the ١٢-month period immediately following the SI's ٥-year maintenance commitment; "Go-Live" means Production Go-Live Acceptance as signed by the Authority.

١٤. GOVERNANCE & COMPLIANCE

١.٦٦. Audit & Oversight: The Authority reserves the right to conduct or commission independent audits at any time, covering infrastructure, application security, development practices, and subcontractor performance. The Contractor shall provide full access to relevant documentation, environments, and staff during such audits. Any identified non-conformities must be addressed through a corrective action plan with defined timelines, and failure to comply shall constitute a material breach.

١.٦٧. International Certifications: The Contractor shall maintain alignment with internationally recognized standards, including ISO/IEC ٢٧٠٠١ (information security management), and PCI-DSS (for payment systems). Where formal certification is not held, the Contractor must demonstrate equivalent controls and commit to achieving certification within an agreed timeframe. Evidence of certifications, audit reports, or control equivalency must be provided during mobilization and maintained throughout the contract term.

١٥. LEGAL AND REGULATORY COMPLIANCE

The system must respect Lebanese laws and regulations related to vehicle registration, driver licensing, data protection, and e-transactions. For instance:

١.٦٨. Records Retention Schedule. Definitive retention periods for datasets and logs shall be set in an Authority-approved Records Retention Schedule (RRS) during mobilization. The system shall provide per-class configurable retention (hot/archive/WORM) and legal-hold. Until the RRS is issued, the solution shall apply Interim retention shall follow the Authority's provisional RRS addendum; the system must allow immediate parameterization without code changes.

١.٦٩. It shall enforce all rules in the Lebanese Traffic Law (Law ٢٤٣/٢٠١٢ and its amendments) regarding licensing conditions, vehicle regulations, fine amounts, point system, categories of vehicles and licenses, etc. The bidders shall familiarize themselves with these legal requirements.

١.٧٠. The Contractor shall comply with all applicable Lebanese laws and regulations, including but not limited to:

١.٧٠.١. Law No. ٢٤٣/٢٠١٢ (Traffic Law) and its amendments.

١.٧٠.٢. Law No. ٨١/٢٠١٨ on Electronic Transactions and Personal Data, including principles of law fulness, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.

١.٧٠.٣. Personal data processing shall be documented via a Data Protection Impact Assessment (DPIA) and Records of Processing Activities (RoPA) prior to go-live. Cross-border transfers (if any) require the Authority's prior written approval and shall follow Law ٨١/٢٠١٨ restrictions. Data subject rights (access, rectification, objection where applicable) shall be supported via auditable workflows within the system. Electronic transactions and signatures: digital signatures are to be used (for notary approvals, for example), they must conform to any Lebanese e-signature law or, if absent, to recognized standards so that they are legally admissible.

١.٧٠.٤. Retention of records and audit logs shall align with legal mandates (for example, keep data for X years). The system's archiving strategy shall reflect any such requirements.

In summary, the general requirements ensure the system is built on a solid, modern foundation that is interoperable, user-friendly, and prepared for future needs. Bidders must address each of these aspects in their technical proposals, confirming how their solution meets or exceeds these standards.

١٦. TECHNICAL & SECURITY REQUIREMENTS

Security is paramount for a system that will hold millions of records on citizens and vehicles, handle financial transactions, and potentially be accessible over the internet. The system must incorporate robust security measures at all levels (application, data, network, and physical) and conform to international security best practices and standards. Below are the security and technical compliance requirements:

١.٧١. **Biometric Lawful Basis & Privacy Controls:**

Processing of biometric identifiers (fingerprints, face images/templates, signatures) shall comply with Law No. ٨١/٢٠١٨. The Contractor shall deliver, prior to UAT, a Data Protection Impact Assessment (DPIA) and Records of Processing Activities (RoPA) covering purposes, data minimization, retention, access controls, and data subject rights. Biometric data shall be encrypted at rest using HSM-protected keys; access is strictly role-scoped and audited.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

Retention periods and deletion criteria (e.g. upon license expiry plus RRS period) are configurable and enforceable system-wide. Cross-border transfers are prohibited without prior written approval of the Authority.

١.٧٢. **Authentication and Access Control:**

The system shall enforce secure authentications for all users. Internal users (Authority staff and admins) will have individual accounts with strong password policies (minimum length, complexity, expiration, history to prevent reuse). Support for Multi-Factor Authentication (MFA) is required for sensitive access (at least for administrative accounts and any remote access). Public users (citizens) registering on the portal/app shall go through a verification process (e.g. verifying mobile number/email via OTP, or using national digital ID if available) to prevent fraudulent accounts. Role-Based Access Control (RBAC) must be implemented, ensuring each user role only accesses the functions and data necessary for their job. There shall also be an ability to define fine-grained permissions (for example, a user can view data but not edit, or can initiate a process but a supervisor must approve). All access and actions must tie back to a user identity for accountability.

Biometric workstation sign-in (Biologin). Staff workstations and thin clients shall support WebAuthn/FIDO٢ or platform biometrics (e.g. Windows Hello/Touch ID) for interactive login with MFA. Shared accounts are prohibited. Device IDs are bound to user sessions and recorded in the audit log.

Security Protocols & Cryptographic Controls

- Transport security: TLS ١.٣ preferred (TLS ١.٢ only where strictly required). Enable HSTS for web properties and enforce modern cipher suites.
- Mutual auth: Use mTLS for service-to-service and external partner APIs where applicable.
- Authentication: Support FIDO٢/WebAuthn (platform security keys) for staff/admin portals; TOTP as fallback. Public portal to support OTP/SMS plus optional national e-ID when available.
- Secrets management: No secrets in code or CI logs. Centralized vault with rotation, leasing, and audit.
- Key Management (On-Prem, No Cloud). All private keys shall reside in Authority-owned Hardware Security Modules (HSMs) located in Authority data centers; keys are non-exportable. The Contractor shall implement an Authority-operated PKI with an offline Root CA and HSM-protected Issuing CAs. Application certificates must auto-renew and rotate

at least every ٩٠ days; data-at-rest keys must rotate at least every ١٨٠ days using envelope encryption. Provide automated workflows, monitoring, and alerts for expiries/rotations. Conduct an annual key ceremony under dual control (M-of-N) with signed minutes and immutable access logs. No use of public cloud KMS/PKI or vendor-hosted key custody is permitted.

- App security headers & hardening: Content Security Policy (CSP), X-Frame-Options/Frame-Ancestors, X-Content-Type-Options, and secure cookies; CSRF protection and strict input validation.
- Supply-chain security: Provide signed SBOM (CycloneDX) per release; perform SCA and container image scans; attest build provenance (target SLSA level as agreed) and patch third-party components per remediation SLAs.
- Crypto modules: Use well-vetted libraries; FIPS-validated modules where available on chosen platform.

١.٧٣. **Data Encryption and Protection:**

All sensitive data stored in the system (personal information, license details, vehicle information, biometrics, etc.) shall be protected. The database shall encrypt sensitive fields or use full-disk encryption on the storage. In particular, any stored biometric data (fingerprint templates, photos, signatures) must be encrypted or hashed as appropriate. Data in transit must always be encrypted using protocols like HTTPS/TLS for web traffic and VPN/IPSec for any connections between sites (e.g. branch offices connecting to the central server). If smart cards (driving license, vehicle registration) store data on a chip, that data shall be protected (e.g. secure access module, PIN or cryptographic security to prevent cloning). The system shall also implement measures against common web security threats: use of prepared statements/ORM to prevent SQL injection, input validation to prevent cross-site scripting (XSS), CSRF protection tokens for web forms, etc. Security testing (vulnerability assessment and penetration testing) will be required before going live.

١.٧٤. Audit Logging and Monitoring:

١.٧٤.١. The system SHALL capture and retain detailed audit events for at least: authentication attempts (success/failure), session lifecycle, privilege elevation, data creation/modification/deletion, configuration changes, approvals/rejections, financial transactions, document/DMS access, export/downloads, API calls (including caller/client ID), and administrative actions across OS, DBMS, middleware, network and application layers.

١.٧٤.٢. Secure Collection & Transport. All components SHALL forward logs in near real-time to a centralized log-collection service using mutually authenticated TLS (mTLS) with certificate pinning. Agents and/or syslog shall include monotonic sequence IDs, host/device IDs, and precise timestamps; NTP/PTP clock drift SHALL be monitored and alerted on (>٥٠٠ ms).

١.٧٤.٣. Immutable Storage & Integrity. Audit logs MUST be written to append-only, tamper-evident storage (WORM or equivalent) with hash chaining and periodic signed checkpoints (e.g., daily). Integrity metadata (e.g., SHA-٢٥٦ digests, Merkle roots) SHALL be anchored and preserved. Deletion, modification, or truncation of audit records is technically and procedurally prohibited; legal hold is supported.

١.٧٤.٤. Segregation of Duties (SoD). The logging/SIEM platform SHALL be operated on a logically and administratively separate system, with a distinct admin team and separate credentials from application/infra administrators. Application/infra admins MUST NOT have rights to delete, alter, or stop audit ingestion or retention. All actions on the logging platform itself are audited. "Break-glass" access requires dual control (maker-checker, M-of-N) with automatic alerts and post-event review.

١.٧٤.٥. Physical/Logical Separation & Replication. The primary log store SHALL reside on infrastructure separate from production application hosts; ideally a different physical location. A LIVE copy of all audit streams SHALL be forwarded to the DR site (RPO ≤ ١٥ minutes) and may additionally be forwarded to a supervising authority sink, subject to law and data-sharing agreements. Store-and-forward buffering handles link outages; dropped-log rate ≤ ٠.٠١٪ monthly.

١.٧٤.٦. Retention & Access Control. Retention follows the Records Retention Schedule and, until finalized, the interim policy (ref. §١٥). Access to audit data is least-privilege, read-only for auditors, and time-boxed; views containing personal data support masking. Lower environments receive redacted/synthetic logs. All access to logs is itself logged.

١.٧٤.٧. Monitoring, Detection & Alerting. The logging platform SHALL integrate with a SIEM or include equivalent correlation/UEBA to detect brute-force attempts, credential misuse, data exfiltration patterns, privilege anomalies, disabled logging agents, integrity check failures, and clock drift. Real-time alerts are delivered to the Authority SOC/NOC with on-call escalation per §١.٣٧.

١.٧٤.٨. Verification & Auditability. Quarterly immutability drills SHALL verify hash chains/checkpoints end-to-end. Any integrity discrepancy triggers incident response.

Evidence packs (hash manifests, signatures, access logs) are produced on request for investigations and external audits.

١.٧٤.٩. KPIs & SLAs. Log ingestion availability ≥ ٩٩.٩٪/month; end-to-end delivery success ≥ ٩٩.٩٥٪; alert dispatch latency P٩٥ ≤ ٦٠ seconds; maximum clock skew ≤ ٥٠٠ ms; integrity verification success ١٠٠٪ or incident declared.

١.٧٥. **Data Loss Prevention (DLP):**

The system shall implement Data Loss Prevention (DLP) controls to protect sensitive data in line with Law ٨١/٢٠١٨ and international standards. DLP shall apply across all channels — databases, APIs, documents, portals, and endpoints — to prevent unauthorized access, exfiltration, or misuse.

Key capabilities include:

- Policy Enforcement: Data classification (public, internal, confidential, restricted) with rules blocking or flagging unauthorized transfers (e.g. bulk downloads, unencrypted exports, removable media use).
- Monitoring & Alerts: Real-time detection of anomalies (by role, device, or location), with violations logged in the central audit trail and surfaced to SIEM dashboards.
- Encryption Alignment: All DLP policies shall complement existing encryption standards to ensure data remains unreadable if intercepted.
- Compliance & Reporting: DLP dashboards and periodic reports shall support regulatory audits, incident review, and continuous improvement of controls.

١.٧٦. **Compliance with Security Standards:**

The solution shall align with international standards such as ISO/IEC ٢٧٠٠١ for information security management and OWASP Top ١٠ guidelines for web application security. While formal certification may not be required for the solution itself, the development practices and architecture shall reflect these standards. If the bidder will host or handle data during development, their processes shall be compliant with ISO ٢٧٠٠١ or equivalent. The data center security (physical and network) shall meet Tier-appropriate standards. Personal data protection measures shall be in line with GDPR principles , ensuring confidentiality, integrity, and availability of data. Bidders shall detail their approach to secure coding and testing in their proposal.

١.٧٧. **Network Security:**

The system's network architecture must be secure by design. The servers hosting the application and database shall reside in a secure network zone, behind firewalls that restrict access only to

necessary ports and services. A demilitarized zone (DMZ) shall be used for any public-facing services (like the web portal) with an application firewall to filter malicious traffic. All connections from the DMZ to the internal network shall be minimized and monitored. If branch offices or external centers connect to the central system, they must do so over secure VPN connections or via dedicated leased lines with encryption. Wireless networks (if any, e.g. at a service center) shall not have direct access to the system network without proper firewalls and authentication. In essence, a defense-in-depth approach must be taken: firewalls, intrusion detection/prevention systems (IDS/IPS), anti-malware on servers, and regular vulnerability scanning of the network.

١.٧٨. **Data Backup and Recovery Security:**

Backups of the system data (and documents) must be performed regularly (daily incremental, weekly full, or as agreed in SLA) and stored securely. Backup data shall also be encrypted, especially if stored off-site or on removable media. Access to backup repositories must be restricted to authorized personnel. The recovery procedures shall be tested periodically (disaster recovery drills) to ensure data integrity and minimal downtime in case of a major incident. Additionally, the system shall have transaction logging such that in case of a minor failure, no data is lost.

In addition, restore of backup data media shall be tested on a separate onsite test environment every six (٦) months, with signed reports and corrective actions tracked.

١.٧٩. **High Availability and Continuity Measures:**

From a technical perspective, the system shall support clustering or failover for critical components. For example, using a database cluster or failover instance so that if the primary database goes down, a secondary can take over (with minimal switchover time). Similarly, multiple application servers behind a load balancer can ensure service continuity even if one server fails. The design shall eliminate single points of failure in hardware and in software. Bidders shall propose an architecture that targets near-zero data loss and quick recovery, aligning with an RTO (Recovery Time Objective) and RPO (Recovery Point Objective) that will be defined by the Authority (for example, RTO of a few hours and RPO of minutes).

١.٨٠. **Physical Security and Environmental Controls:**

Although largely an infrastructure concern, the system design shall account for physical security needs – such as ensuring that enrollment devices (cameras, fingerprint readers) are used in controlled environments to prevent identity fraud, and card printing equipment is in secure locations to prevent theft or misuse of blank licenses or plates. The system shall also require login/authentication on all client workstations to ensure only authorized staff use it at counters.

١.٨١. **Privacy and Data Access Policies:**

The system shall incorporate privacy-by-design principles. Personal data fields shall be masked or hidden from users who don't need to see them. For example, an inspector verifying a vehicle might not need to see the owner's full ID number or personal details – the system could just show necessary info (like registration validity) to them. Only higher-level users can access full profiles. There shall be functionality to mark certain profiles or records as sensitive (for example VIP users or cases under investigation) such that only specifically cleared personnel can view them. The system shall also allow the Authority to extract or delete personal data if required by any future data protection regulations (right to be forgotten, etc., where applicable for people who no longer have any active records).

١.٨٢. **Digital Signature and Document Security:**

If the system generates electronic documents (like e-registration certificates, e-receipts, or if it sends digital records to other entities), these shall be cryptographically signed to ensure authenticity and integrity. For example, a PDF of a car registration extract given to a user online might carry a QR code or a digital signature that law enforcement or another agency can validate to ensure it hasn't been tampered with. The system shall integrate with a Public Key Infrastructure (PKI) for issuing and verifying such signatures. Likewise, any integration with notaries or physicians where they "sign" off on something shall utilize certified digital signatures or credentials so that those approvals are legally binding and traceable.

١.٨٣. **Mobile App & Digital Credential Security:**

- Mobile app hardening. Implement anti-tamper/obfuscation, jailbreak/root detection, certificate pinning, OS attestation (e.g. Apple Device Check/Attestation), secure key storage (Secure Enclave/Keychain), and runtime hooking detection. Block app execution on compromised devices.
- Digital cards with PKI. Digital driver's license and vehicle registration displayed in the app shall be digitally signed using Authority PKI (private keys secured in HSM). QR codes used for roadside checks must carry a detached/offline-verifiable signature; police apps verify using the published Authority public key even without connectivity.
- Device/account binding. Bind digital credentials to user account and device; support remote revoke/rotate, session timeout, and step-up authentication for sensitive actions.
- Mutual TLS. All app-API calls use mTLS; tokens are short-lived with DPoP/PKCE where applicable.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

In summary, the system shall be secure by design and by default, leaving no gaps for potential breaches. Given the reliance on digital services, trust in the system is critical – citizens and stakeholders need confidence that their data is safe and transactions are secure. The selected vendor will need to demonstrate a strong track record in secure system design and commit to ongoing security support (patching, updates) as part of maintenance.

١٧. PERFORMANCE REQUIREMENTS

١.٨٤. Availability (core services): ≥ ٩٩.٩٠٪ per calendar month (excluding approved maintenance windows ≤ ٤ hours/month announced ≥ ٧ days in advance).

١.٨٥. Performance (interactive): P٩٥ ≤ ٢.٠s and P٩٩ ≤ ٥.٠s for read operations ≤ ١٠٠ KB; create/update operations P٩٥ ≤ ٣.٠s during normal hours at stated peak loads. P٩٥ ≤ ٣.٠s during normal hours at stated peak loads.

١.٨٦. API performance & reliability: Sustain ≥ ٢٠٠ TPS with burst ≥ ٦٠٠ TPS over ٦٠s, non-٤xx error rate ≤ ٠.٥٪. Vendor to provide capacity tests and reports.

١.٨٧. Disaster Recovery Targets: RTO ≤ ٤ hours; RPO ≤ ١٥ minutes.

١.٨٨. Canned dashboards must load in ≤ ٥s P٩٥ for defined filters; ad-hoc queries run in governed workspaces with workload isolation. Materialized UTN-centric views are refreshed per SLA and include data-freshness indicators.

١.٨٩. UTN-centric lookups: Provide UTN-centric materialized views and indexes for high-volume lookups (≤ P٩٥ ٢.٠s at peak).

١.٩٠. Mobile App KPIs: Crash-free sessions ≥ ٩٩.٥٪ monthly; cold start ≤ ٢.٥s on reference mid-tier devices; offline mode for credential verification (QR/signature check) with secure sync on reconnect.

١.٩١. The system must be capable of handling current transaction volumes and projected growth over at least the next ١٠ years, including:

١.٩١.١. Active vehicles: ٤,٠٠٠,٠٠٠; annual renewals: ٣,٢٠٠,٠٠٠; peak-day renewals: ٥٠,٠٠٠.

١.٩١.٢. Licensed drivers: ٣,٥٠٠,٠٠٠; theory/practical tests per day: ٢,٠٠٠

١.٩١.٣. Concurrent internal staff users (peak): ٥٠٠; portal concurrent sessions (peak): ٦,٠٠٠.

١.٩١.٤. Peak payment authorizations per minute: ٤٠٠

١.٩١.٥. Average document/image size: ٠.٧٥ MB; daily ingest: ١٥ GB

١.٩١.٦. Retention: audit logs hot ٤٠٠ days, archive ٧ years WORM; transaction artifacts ١٠ years; CCTV ٩٠ days unless case-locked.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

١.٩١.٧. Performance & Resilience Testing: Load and stress tests shall use production-like mixes (read/write ratios, peak burstiness, feature flags enabled), realistic think times, and anonymized/masked datasets. Tests must cover failover under load, dependency throttling, and rollback during canary/blue-green deployments. Results (including resource headroom ≥ ٣٠٪ at peak) are acceptance-gated with artifacts shared to the Authority.

١٨. DATA CENTER AND INFRASTRUCTURE REQUIREMENTS

١.٩٢. The bidder shall size hardware, licenses, and capacity using the baseline volumes specified in the "PERFORMANCE REQUIREMENTS" section. Vendors shall provide a capacity model, test data generators, and evidence of headroom ≥ ٣٠٪ at peak.

١.٩٣. The solution will be deployed in the Authority's data center, and must include all necessary hardware, networking, and infrastructure to ensure reliable operations across all regional branches and any new service centers. This section details the requirements for the Data Center, connectivity, and related infrastructure components:

١.٩٤. Primary Data Center Setup: The main servers hosting the system (application servers, database servers, etc.) will reside in a primary Data Center (DC) designated by the Authority (for example, at the central headquarters or a government IT center). The bidders shall propose hardware specifications to handle the system's load with redundancy:

١.٩٤.١. On-Premises Only / Data Residency. All processing, storage, backups, logs, telemetry, and build artifacts shall be hosted on-premises in Lebanon under Authority control. Public cloud services are not permitted for production, DR, or telemetry. Any external connectivity (e.g. payment gateways, SMS) must avoid exporting personal data beyond what is legally required and shall comply with Lebanese regulations.

١.٩٤.٢. Server Hardware: Enterprise-grade servers for application and web services (potentially running in a virtualized environment or containerized setup for microservices) and robust database servers. These shall have high-performance CPUs, ample RAM, and fast storage (SSD-based) to meet the performance needs. The capacity shall be planned with at least ١٠ years growth in mind (number of vehicles, users, etc. expanding).

١.٩٤.٣. Storage: A Storage Area Network (SAN) or similar solution may be required for handling the large volume of data (including the document archives like scanned images). Storage shall be redundant (RAID configurations) and scalable. For archival documents (which could be very large in aggregate size), cost-effective but reliable storage tiers shall be suggested.

١.٩٥. Networking Equipment: Firewalls, switches, load balancers, and intrusion detection systems shall be provided if not already in place. Network infrastructure must support segregating traffic (public portal vs internal traffic) and provide quality of service to critical operations. Gigabit or higher bandwidth connectivity within the data center is expected between servers and storage.

١.٩٦. Virtualization/Containerization: It is encouraged to use virtualization (e.g. VMWare, Hyper-V) or container orchestration (Docker/Kubernetes) to maximize resource usage and simplify deployment. Bidders shall specify if they plan to use virtual machines or containers and detail the management of those (for instance, a Kubernetes cluster for microservices).

١.٩٧. Operating Systems and Software Licenses: on-premise deployment with necessary operating system and database software licenses. The vendor shall include all required licenses in their proposal. The database must meet performance and support criteria.
All OS, database, middleware, security, and application licenses shall comply with the "Software License Term, Renewal & Co-Termination" clause in Intellectual Property & Licensing, including lifetime/perpetual preference, six (٦) years of continuous coverage from Go-Live, and Authority ownership of all entitlements.

١.٩٨. Disaster Recovery (DR) Site: In addition to the primary DC, a Disaster Recovery site shall be established to take over in case the primary site becomes unavailable (due to power failure, natural disaster, etc.). The DR site can be a government-provided secondary data center in a different location separate from the primary. Requirements:

١.٩٨.١. DR Architecture & Replication. The Bidder shall deploy a warm-standby DR environment in a facility separate from the primary. Databases shall use asynchronous replication targeting RPO $\leq$ ١٥ minutes; application artifacts and object stores shall replicate on an RPO $\leq$ ٣٠ minutes schedule. End-to-end RTO $\leq$ ٤ hours via documented runbooks and semi-annual switchover drills. No public cloud is permitted; all replicas remain on-prem.

١.٩٨.٢. The system shall support failover to DR. If the primary system goes down, the DR system shall be able to come online and serve at least critical functions within a short time. Bidders shall describe their DR strategy, including how data is replicated (database mirroring, log shipping, storage replication, etc.) and how failover/failback is managed (manual vs automatic).

١.٩٨.٣. Regular drills shall be possible: e.g. switching to DR in a test scenario to ensure it works as intended.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

١.٩٩. Branch and Center Connectivity: All branch offices (the existing ٧ regional offices and any additional offices or authorized private centers in the future) need to connect to the central system. The network requirements include:

١.٩٩.١. A secure WAN (Wide Area Network) connecting all sites. This could be via MPLS links provided by a telecom provider. The Authority will coordinate telecom needs, but the system shall be capable of operating over the provided network. Minimum bandwidth and latency requirements for satisfactory performance shall be stated by the bidder (taking into account operations like uploading documents, real-time queries, etc.).

١.٩٩.٢. Redundancy in connectivity for important sites (for example, the central site shall have dual internet providers or links; key large branches might have a backup ٤G/٥G or secondary link in case the primary fails).

١.٩٩.٣. All data exchanges between branches and center must be encrypted (VPN tunnels or equivalent security). The system's design (thin client web-based vs local processing) will impact bandwidth use; a web-based system mostly sends screen data and is suitable for WAN.

١.٩٩.٤. The system shall also support remote connectivity for authorized users (with VPN and appropriate authentication), for example if certain administrators need to connect from the Ministry or if a roaming inspector submits a report from the field.

١.١٠٠. Infrastructure at Branches/Centers: The RFP includes provision of hardware to modernize the branch offices and any new service centers:

١.١٠٠.١. CCTV & Evidence Retention. Record continuous CCTV at counters and lane exits with tamper-evident storage linked to transactions. Apply retention schedules and restricted access with audit.

١.١٠٠.٢. Workstations and Peripherals: Each service counter at a branch or center will need a PC or terminal for the staff to use the system, along with devices like document scanners (for scanning application papers into the archive), document printers for receipts or certificates, signature pads (to capture digital signatures from applicants), and biometric enrollment devices (fingerprint readers and digital cameras for capturing applicant photo) as needed for driving license processing. The vendor shall specify quantities and models based on the typical workflow at each site. Existing hardware (if any from current system) shall be assessed – some may be reused if compatible, but assume new equipment for reliability.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

١.١٠٠.٣. Network and Power: Each site require network switches, routers, and firewall appliances to connect to the central system securely. Also, a UPS (Uninterruptible Power Supply) for each critical computer or a centralized UPS for the site to allow graceful shutdown during power cuts (given power instability issues in some areas). The vendor shall include a plan for stable power at least for the critical equipment (not necessarily full site generator unless specified by Authority).

١.١٠١. **Kiosks** : The system shall have the capability to work with self-service kiosks if the Authority decides to deploy kiosks in public places (like malls or large centers) for certain tasks (e.g. paying fees, printing or reprinting a driving licence or vehicle registration card, and issuing standard confirmations), as and when explicitly requested in writing by the Authority.

١.١٠٢. Import & Logistics Readiness (Vignette Ecosystem)

The SI shall submit with the bid an Import Readiness Plan covering: BoQ of sticker media, encoders/printers, handhelds/fixed readers.

١.١٠٣. Card Issuance and Personalization Equipment: The vendor must provide all needed if not present hardware for printing and encoding the smart driving license cards and vehicle registration cards at the required locations. This likely includes card printer/encoders, lamination or laser engraving equipment (depending on card technology used), print servers and software. Similarly License plate manufacturing equipment will be provided and operated by the plate contractor; the SI supplies the digital control/orchestration and integrations.

١.١٠٤. Environmental Controls and Physical Security: The Data Center must adhere to standards for physical security and environment:

١.١٠٤.١. Access Control: Only authorized personnel shall have physical access to servers. Use of access cards, biometric access to server rooms, and CCTV monitoring is recommended. While the Authority will ensure the facility security, the bidder shall design racks and equipment with lockable cabinets where appropriate.

١.١٠٤.٢. Power and Cooling: Adequate cooling (air conditioning) for server rooms, plus backup power (UPS and generator support) are required. The system's critical components shall be protected from power surges and outages. The Authority's site likely already has backup generators, but the bidder shall confirm and ensure the UPS sizing covers at least the interim until generators kick in.

١.١٠٤.٣. Fire Safety: Server rooms shall have fire suppression (e.g. inert gas systems) and smoke detection. While this might be outside the software scope, any additional

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

requirement for protecting specialized equipment (like card printers that might be sensitive) shall be noted.

١.١٠٤.٤. Rack Space and Cabling: All hardware shall be rack-mounted where possible. Cabling shall be well-organized and labeled. Bidders must provide detailed infrastructure diagrams showing how everything will be connected.

١.١٠٥. Infrastructure Documentation: The vendor must provide complete documentation of the infrastructure setup. This includes network diagrams, IP schemas, inventory of equipment, and configuration details for all devices (so that the Authority's IT staff can maintain it post-implementation). Training shall be given to the technical team on managing the servers, network, backups, and other infrastructure elements.

Overall, the infrastructure provided shall ensure the system runs smoothly across all locations with minimal downtime. The vendor is expected to deliver a turnkey solution, meaning all necessary hardware and network configuration is part of their scope (unless explicitly stated as provided by the Authority). The solution shall accommodate current needs and be extensible for future expansions (e.g. if more branches are added or transaction volumes increase). Robust connectivity and a strong data center foundation underpin the entire digital transformation effort, making this aspect crucial for success.

١٩. TESTING & QUALITY ASSURANCE

١٩.١. Scope & Principles. The delivered system SHALL undergo comprehensive testing: unit, integration, end-to-end, performance/load, resilience/failover, accessibility, and security. The SI shall support User Acceptance Testing (UAT) by the Authority. No component may enter production without passing all security and quality gates and having an approved rollback plan.

١٩.٢. Independent Security Company (Authority-Commissioned). The Authority SHALL commission, via a separate tender running in parallel with this tender, an independent third-party security company to perform secure code review and greybox penetration testing (PT). The security company shall be organizationally independent from the SI and its subcontractors. Acceptance into production is contingent on written validation by the Authority's security company at the gates defined below.

١٩.٣. Security & Quality Gates (Stop/Go).

Promotion is blocked until the Authority's security company issues a written Pass/Conditional Pass for each gate:

Gate A – Design: Threat modeling for major features; security design review Pass.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

Gate B – Pre-UAT Build: Initial secure code review (SAST/MAST + manual on high-risk areas) and greybox PT; no Critical/High findings open.

Gate C – Pre-Production: Full retest (app, APIs, mobile, infra) on production-parity build; no Critical/High; Mediums mitigated or risk-accepted by the Authority.

Gate D – Major Release/Change: Targeted review + PT on changed scope prior to production rollout.

Emergency fixes may be deployed only with documented compensating controls, CAB approval, and mandatory retest within ١٤ calendar days.

١٩.٤.CI/CD Security Controls. The SI SHALL implement continuous security testing in CI/CD: static analysis (SAST), dynamic analysis (DAST), mobile app security testing (MAST) where applicable, dependency/SBOM scans (SCA), infrastructure-as-code scans, and container image scans. Builds FAIL on Critical issues by policy. SBOM and vulnerability scan reports are provided per release.

١٩.٥.Greybox Penetration Testing Cadence. Independent greybox PT SHALL occur prior to initial go-live, at least annually thereafter, and on major releases. Mobile apps are re-validated on each store-published release that affects security surfaces.

١٩.٦.Performance & Resilience Testing. Each major release SHALL include performance testing at target volumes and burst profiles; results (KPIs, headroom, bottlenecks) are included in release notes. Failover, throttling/circuit-breaker behavior, and rollback are exercised under load.

١٩.٧.Access & Artifacts for Validation. The SI shall provide to the Authority's security company: architecture/HLD/LLD, threat models, API specs, SEC/UAT access, seeded test data, read-only access to source repositories/pipelines, SBOMs, and representative builds (web, mobile, services). Materials are covered by NDA and used solely for validation.

١٩.٨.Findings, Remediation & Retest. Severity thresholds: Critical/High MUST be remediated and retested prior to promotion; Medium MUST be remediated or have approved compensating controls with formal Authority risk acceptance; Low/Info tracked to closure. Remediation SLAs align with §٢٠.١.١٠٨.٧ unless stricter windows are set for pre-prod gates. The SI bears retest costs for regressions.

In addition, the SI shall proactively identify, report, and remediate any cybersecurity gap or vulnerability discovered at any stage of the project or during operations—including design flaws,

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

configuration weaknesses, or newly disclosed threats—at no additional cost to the Authority.

١٩.٩. Evidence & Deliverables. The SI SHALL deliver test plans, scripts, datasets, and reports for all test types; the Authority's security company SHALL deliver executive and technical reports, PoC evidence, and a signed validation letter per gate. Gate outcomes and ticket IDs MUST map in the Requirements Traceability Matrix.

١٩.١٠. Governance & Approval. Authority Technical Committee Approval is required for all modules, configurations, updates, pilots, phased go-lives, and release trains. No pilot or phased rollout may proceed without written sign-off. No production deployment may occur without passing all gates and having an approved rollback plan.

٢٠. SERVICE LEVELS, WARRANTY, AND ACCEPTANCE

١.١٠٦. Warranty, Maintenance & Commitment.

١.١٠٦.١. The offer shall include one (١) year comprehensive warranty/maintenance for all HW & SW (central and regional), with parts, labor, and preventive maintenance.

١.١٠٦.٢. The Bidder shall submit an original signed and stamped commitment letter to provide support and maintenance services to the Authority for a minimum period of four (٤) years from contract signature.

١.١٠٦.٣. Service Level Targets: As defined in the "PERFORMANCE REQUIREMENTS" section, the system shall meet availability ≥ ٩٩.٩٠٪, interactive P٩٥ ≤ ٢.٠s, API ≥ ٢٠٠ TPS sustained, RTO ≤ ٤ hours, and RPO ≤ ١٥ minutes.

١.١٠٦.٤. Security remediation SLAs: Critical CVEs ≤ ٧٢h; High ≤ ١٠ business days; Medium ≤ ٣٠ business days unless compensating controls are accepted in writing.

١.١٠٦.٥. Business Continuity Exercises

١.١٠٦.٦. In addition to quarterly tabletop exercises, the Contractor shall perform semi-annual live DR switchovers (warm site) during agreed windows, validating RTO/RPO, application health, and data reconciliation. Each exercise produces signed reports, issues, and tracked corrective actions. Passing the first live switchover is an acceptance gate for production expansion.

١.١٠٧. Acceptance Gates (must all pass):

١.١٠٧.١. Factory & System Integration Tests (traceable to requirements), including witnessed Factory Acceptance Tests (FAT) at the manufacturer/vendor site prior to shipment, with signed protocols.

١.١٠٧.٢. Performance/Load Test meeting the targets above at Authority-agreed volumes.

١.١٠٧.٣. Vignette Pilot Acceptance: A ٣٠-day field pilot at two branches and two road lanes (urban + peri-urban). Success criteria: lane read success ≥ ٩٥٪, static read success ≥ ٩٩٪, barcode first-pass ≥ ٩٩.٥٪, and ≤ ٠.٢٪ spoilage. Failure requires vendor remediation and re-pilot.

١.١٠٧.٤. Independent third-party penetration test with all Critical/High findings remediated or risk-accepted by the Authority.

١.١٠٧.٥. UAT sign-off, pilot sign-off, and rollback plan validated in rehearsal.

١.١٠٧.٦. As-built documentation, SBOMs, and runbooks delivered and approved

١.١٠٨. Program Governance & Change Control

The Contractor shall operate under a formal governance model approved by the Authority that includes:

- a Product Owner, CISO, DPO, and Architecture Review Board appointed by the Authority;
- a Change Advisory Board (CAB) with impact tiers (Standard, Normal, Emergency), lead times, and rollback criteria; and
- a living Configuration Management Database (CMDB) covering services, environments, dependencies, and owners. All scope, configuration, and regulatory changes flow through the CAB with assessed security impacts and business justifications.

٢١. RISK MANAGEMENT

The Contractor shall establish and maintain a structured risk management framework throughout the engagement. Risks shall be identified, assessed, monitored, and mitigated across all phases of the project, covering technical, operational, security, compliance, and delivery domains.

- Risk Register: The Contractor shall maintain a continuously updated Risk Register documenting identified risks, their likelihood and impact, assigned owners, and agreed mitigation actions. The Risk Register shall be shared with the Authority on a monthly basis or upon request.
- Classification and Prioritization: Risks shall be categorized by severity (Critical, High, Medium, Low) with defined escalation paths. Critical risks must be immediately reported to the Authority along with recommended mitigation or contingency measures.

- Mitigation and Contingency: Each risk shall include defined mitigation steps and fallback procedures to ensure minimal impact on Authority operations.
- Integration with Governance: Risk management activities shall be aligned with the Program Governance and Change Control processes to ensure that emerging risks related to scope changes, regulatory updates, or third-party dependencies are promptly addressed.
- Reporting and Review: The Contractor shall provide periodic risk reports, trend analysis, and updates on mitigation effectiveness as part of overall project status reporting. Risks not resolved within agreed timelines shall trigger escalation to the Authority.

٢٢. IMPLEMENTATION TIMELINE

The Contractor shall submit a detailed implementation plan within four (٤) weeks of contract signature, subject to Authority approval. The plan shall include:

- Mobilization phase (team onboarding, discovery, environment setup).
- Design and Architecture (HLD/LLD, data models, integration specs).
- Development & Configuration (modular delivery with clear milestones).
- Testing (unit, integration, UAT, security, and performance).
- Training & Knowledge Transfer (Authority staff, notaries, inspectors, branch operators).
- Go-Live & Transition (production cutover, stabilization period).
- Each phase shall have defined deliverables, acceptance criteria, and target completion dates. Deviations greater than two weeks require a formal Change Request to the Authority with justifications and mitigation measures.

ملحق رقم (١١) شروط اضافية يجب التقيد بها

١. حقول التتبع والتدقيق(Audit Fields)

يجب أن يتضمن كل جدول تشغيلي في قواعد البيانات الحقول التالية:

CreatedBy, CreatedOn, ModifiedBy, ModifiedOn, DeletedBy, DeletedOn, IsDeleted.

٢. سياسة الحذف اللطيف(Soft Deletion)

يُحظر الحذف الدائم لأي سجل. يتم الحذف عبر تعيين الحقول أعلاه ومنها IsDeleted وتسجيل هوية المنفّذ وتاريخه. لا يُسمح بالحذف الفيزيائي إلا بقرار خطّي من اللجنة التقنية وبأداة ترحيل/نسخ مُدارة.

٣. ضبط تغييرات قاعدة البيانات في بيئة الإنتاج

يُمنع تنفيذ أي Direct Scripts على الإنتاج دون طلب تغيير (Change Request) مُعتمد وفق مبدأ Maker–Checker مع خطة تراجع (Rollback) وهوية تذكرة عمل.

٤. تسجيل وتنفيذ السكربتات

تُسجّل جميع عمليات DDL/DML على الإنتاج وتؤرشف مع التحقق (Checksum) وهوية المنفّذ ووقت التنفيذ لغايات المراجعة اللاحقة.

٥. الإدارة مالكٌ للمنتج

تملك الإدارة كامل حقوق الملكية الفكرية لجميع المخرجات. تُمنح الإدارة وصولاً كاملاً وفورياً إلى المصدر البرمجي، وخطوط النشر (Deployment Pipelines) ، والآلات الافتراضية والخوادم ذات الصلة، دون قيود (ارتباطاً بمواد القابلية للصيانة في المادة ٣٣).

٦. ترقيم الكود وقواعد البيانات

يُدار الكود عبر نظام Version Control (Git) بإستراتيجية فروع واضحة؛ وتُدار تغييرات قواعد البيانات عبر أداة ترحيل مُدارة تضمن تتبّع الإصدارات وإمكانية التراجع.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

٧. **تعدد البيئات**

حدٌّ أدنى من البيئات Development و Staging/UAT و Sec/Pen,Production تُحجب البيانات الشخصية في البيئات غير الإنتاجية، وتُفصل الحسابات والأسرار بينها، وتخضع الترقية لضوابط CI/CD

٨. **التخطيط والالتزام بالمواعيد**

إبقاء Product Backlog وخارطة طريق و Gantt مُحدّثة طوال مدة المشروع، مع تقارير تقدّم دورية.

٩. **وصول شفاف إلى الكود المصدري**

حصول الإدارة على وصول كامل وفوري إلى جميع المستودعات (القائم وتحت التطوير) وتسليم النسخة المصدريّة عند دخول أي وحدة إلى الإنتاج، ومنع أي Vendor Lock-in .

١٠. **الوصول إلى خطوط النشر (Deployment Pipelines)**

توفير وصول إداري للإدارة إلى جميع خطوط النشر والأسرار/المفاتيح المرتبطة بها، مع توثيق إجراءات التسليم والاستمرارية.

١١. **منع التغييرات الأحادية**

يُحظر أي تغيير مباشر على الإنتاج من طرف واحد. تُنفَّذ التغييرات ضمن إجراءات مُصادَقة ثنائية Maker-Checker وسجل تغييرات رسمي.

١٢. **التوثيق ودليل الاستخدام لكل ميزة**

مطلوب وثائق شاملة لكل ميزة تشمل مخططات انسيابية، دليل مستخدم/مسؤول، مواصفات واجهات (OpenAPI/JSON)، وأدلة تشغيل (Runbooks) .

١٣. **استخدام تقنيات حديثة ومدعومة**

يُحظر استخدام أطر/مكتبات منتهية الدعم أو غير مرخّصة. يُلزم المورّد بتقديم قائمة SBOM ومعالجة الثغرات (CVE) ضمن آجال متفق عليها.

١٤. استبعاد حلول التقارير القديمة

لا تُقبل أدوات تقارير قديمة/غير مدعومة. يجب اعتماد منصة BI/Analytics حديثة ومدعومة مع إمكانات تصدير وآليات تفويض وأمن.

١٥. مراقبة النظام وقابلية الرصد(Observability)

تفعيل Logs و Metrics و Traces و APM مع حدود احتفاظ واضحة وربط بمنصة SIEM وتنبيهات فورية، ومواءمة هذا البند مع المادتين ٣٣-٣٤.

١٦. سياسة السجلات والتدقيق والأرشفة(System & Security Logging)

- **النطاق:** سجلات تطبيقية،(سجلات الأمان AuthN/Z) وتغييرات الصلاحيات ومحاولات الدخول(سجلات البنية التحتية(OS/DB/K٨s/Proxy) ، وسجلات واجهات التكامل (APIs).
- **الشكل والتوقيت:** سجلات منظَّمة بصيغة JSON مع Correlation/Trace IDs وطوابع زمنية UTC متزامنة عبر NTP.
- **المركزية والنقل:** تجميع مركزي ودفع إلى SIEM مع تقارير يومية/أسبوعية/شهرية.
- **السلامة وعدم القابلية للعبث:** اعتماد مخازن Append-Only/WORM أو تجزئة متسلسلة (Hash-Chaining) وإثبات سلام(Integrity Checksums).
- **الخصوصية** :إخفاء/تعمية الحقول الحساسة (PII/PCI) وفق سياسة تصنيف البيانات.
- **الوصول** :صلاحيات قراءة فقط لمجموعات مُدقّقة، مع سجل وصول للسجلات نفسها.
- **مدد الاحتفاظ الدنيا:**
  - سجلات الأمان والتدقيق: طبقة حارّة ≤ ١٢ شهراً، وأرشيف بارد ≤ ٥ سنوات.
  - سجلات التطبيقات والبنية التحتية: طبقة حارّة ≤ ٦ أشهر، وأرشيف بارد ≤ ٣ سنوات.
- **المراجعة والمعالجة:** مراجعة أسبوعية للإنذارات الحرجة وتحليل شهري لاتجاهات المخاطر وخطط معالجة مُوثّقة.
- **التجميد القانوني (Legal Hold):** القدرة على تجميد السجلات محلياً عند الطلب القضائي مع تتبّع كامل.

الجمهورية اللبنانية
هيئة إدارة السير والآليات والمركبات
الرئيس - المدير العام
وزارة الداخلية والبلديات

١٧. أرشفة البيانات التشغيلية وقابلية الاستعادة في قواعد البيانات

- تفعيل سجل معاملات قاعدة البيانات (Transaction Logs) مع استرجاع حتى نقطة زمنية(PITR)
- أرشفة دورية للسجلات التاريخية (Closed/Inactive) إلى أقسام/مخططات أرشيفية مُضغَّطة للقراءة فقط، مع فهارس استرجاع سريعة.
- سياسات احتفاظ بالبيانات وفق المتطلبات القانونية؛ أي شطب/تنقيح نهائي يتم عبر إجراءات مُعتمَدة ومُسجَّلة (Change + Maker–Checker) مع تقرير تدقيق.
- تشفير النسخ الاحتياطية والأرشيفات بمفاتيح مُدارة عبر HSM/KMS ، واختبارات استعادة مُجدولة (≤ مرّتين سنوياً) مع تقارير نجاح.

١٨. إدارة المخاطر وخطة الطوارئ(DR/BCP)

تقديم خطة تعافي كوارث مُجربة دورياً (≤ مرّتين سنوياً) تستوفي أهداف RPO/RTO المُعتمدة، وتشمل قاعدة ١-٢-٣ للنسخ الاحتياطي:

– نسخة تشغيلية في مركز البيانات (وفق المادة ٣٥).

– نسخة مُشفّرة خارج الموقع على وسائط مناسبة (أشرطة/وسائط غير متصلة) في مكان آمن تحدده الإدارة خارج مبنى الدكوانة.

– تسليم نسخة دورية من البيانات للإدارة.

يُلزَم المورّد باختبارات استعادة مُوثّقة للتأكد من صلاحية النسخ.

١٩. سرية البيانات والملكية الفكرية

التزام كامل بحماية السرية والخصوصية وفق القوانين والمعايير، مع تأكيد أن جميع الأكواد والمنتجات الناشئة ملكٌ حصريٌ للإدارة بموجب هذا العقد.

٢٠. المنهجية والاجتماعات والمتابعة

اعتماد مبادئ Agile . للإدارة حق حضور الاجتماعات اليومية واجتماعات متابعة نصف شهرية، مع توثيق القرارات والإجراءات المتفق عليها.

٢١. بيئة اختبار الاختراق والتدقيق الأمني الخارجي(Pentest / UAT-Sec)

- إنشاء بيئة UAT-Sec مُحاكية للإنتاج (بلا بيانات مواطنين حقيقية؛ بيانات مُقنّعة/مُجهّلة) ومعزولة شبكياً، تمرّ عبرها جميع الإصدارات قبل الإنتاج.
- الاختبارات الإلزامية قبل الإصدار SAST و SCA (فحص الاعتمادات والثغرات)، ومسح صور الحاويات، و DAST للتطبيقات والواجهات، وفحوص تهيئة البنية (CIS Benchmarks)، واختبارات أداء أمنيّة أساسية.
- التعاقد مع جهة تدقيق/اختبار اختراق خارجية معتمدة لإجراء Black/Grey Box على: البوابة والموبايل(Android/iOS) ، وواجهات الـAPIs ، والخدمات الخلفية، وأصول الإنفرا و CI/CD.
- التسليمات: تقرير ثغرات مُفصّل) تصنيفCVSS ، أدلة إثباتPoC ، أثر، علاج مقترح + (جلسة قراءة فنية + خطاب إغلاق بعد المعالجة وإعادة الاختبار.
- الحَوْكمة: جدول اختبارات رُبع سنوي على الأقل، واختبار رئيسي قبل كل إصدار كبير، وقياس امتثال علاجات الثغرات، ورفع تقارير موجزة إلى الإدارة.
- النفاذ والأمان: وصول مراقَب قائم على أقل امتياز، وسجلات كاملة لأنشطة شركة التدقيق، ومفاتيح/أسرار مؤقتة تُبطل بعد انتهاء النافذة.