eSign Subscriber Agreement

Issue Date:	15 June 2022
Effective Date:	17 June 2022
Document Identifier:	POL-AGR-SUB-02
Version:	1.0
Document Classification:	**PUBLIC**
Document Status:	**Final**

Latest version of this document will be available at https://www.emdha.sa

1. Definitions and Scope

1.1. emdha eSign CA

The term ‘emdha eSign CA’ refers to the CA entity directly under the BTC LICENSED CA, owned and operated by BTC, and is approved by DGA to be part of the Saudi National Public Key Infrastructure (PKI).
emdha eSign CA is responsible for:

1.1.1 Generation, issuance and distribution of subscriber related trust service certificates and supporting services certificates under the emdha eSign CA;

1.1.2 Revocation or/and suspension of subscriber related trust service certificates and supporting services certificates;

1.1.3 Periodic publication of revocation information in the form of CRL;

1.1.4 Provide certificate revocation information as a OCSP responder

1.1.5 Renew or Re-key of Trust services and other supporting services certificates;

1.1.6 Conduct regular certificate and internal security audits;

1.1.7 Assist in audits conducted by or on behalf of DGA and/or Webtrust for CAs related audits; and

1.1.8 Performance of all aspects of the services, operations and infrastructure related to emdha eSign CA.

1.2 -Trust Services

Trust Services are electronic services that consume digital certificates to provide capabilities for certificate-based authentication, digital signatures, verification, validation and/or preservation for electronic transactions. Trust Services provide and/or enhance integrity, reliability and trust in electronic transactions.

Below is a list of Trust services owned, managed and provided by emdha to be used with the emdha eSign CA.

1.3 eSign Trust Service or Online Signature Service (eSign)

eSign Trust Service enables Signature Interface Providers (SIP) to integrate their digital service platform with emdha eSign CA and thereby facilitate remote online signature facility for their applications, customers and end-users. It is responsible for:

1. Requesting and/or receiving validated subscriber Know Your Customer (KYC) information from a Reliable KYC Agency (RKA);

1. التعريفات والنطاق

1.1. مركزتصديق "إمضاء" للتوقيع الرقمي

يشير المصطلح مركز تصديق "إمضاء" للتوقيع الرقمي الى المركز المملوك بواسطة شركة بُعد للاتصالات ويعمل تحت ادارتها والمعتمد من هيئة الحكومة الرقمية ليكون جزء من البنية التحتية للمفاتيح العامة في السعودية.
ويكون مركز تصديق "إمضاء" للتوقيع الرقمي مسؤولاً عن:

1.1.1 اعداد وإصدار وتوزيع شهادات خدمات الثقة وشهادات الخدمات المساندة الخاصة بالمشترك.
1.1.2 إلغاء او تعليق شهادات خدمات الثقة والشهادات المساندة الأخرى الخاصة ب بالمشترك.
1.1.3نشر معلومات الإلغاء بصورة دورية في شكل نموذج في قائمة الشهادات الملغاة CRL .
1.1.4 تقديم معلومات الغاء الشهادات في شكل بروتوكول حالة الشهادات عبر الانترنت لـ OCSP.
1.1.5 تجديد أو إعادة اصدار مفتاح شهادة الخدمة الموثوقة وشهادات الخدمات المساندة الأخرى.
1.1.6 إجراء مراجعات أمنية داخلية منتظمة.
1.1.7 المساعدة في تنفيذ المراجعات التي يتم إجراؤها بواسطة أو بالنيابة عن هيئة الحكومة الرقمية و / أو (Webtrust) فيما يتعلق بالمراجعات الخاصة بمراكز التصديق الرقمي، و
1.1.8 تنفيذ كافة أوجه الخدمات والعمليات والبنية التحتية المرتبطة بـ " مركز تصديق "إمضاء" للتوقيع الرقمي

2.1. خدمات الثقة

خدمات الثقة هي خدمات إلكترونية تستخدم الشهادات الرقمية لتوفير إمكانيات التصديق المبني على الشهادة والتوقيع الرقمي والتحقق و حفظ المعاملات الإلكترونية. إن خدمات الثقة توفر النزاهة والمصداقية والثقة في المعاملات الإلكترونية.

أدناه قائمة بخدمات الثقة المملوكة والمدارة والمقدمة بواسطة "إمضاء" والتي تستخدم مع مركز تصديق "إمضاء" للتوقيع الرقمي

3.1 خدمة الثقة للتوقيع الرقمي أو خدمات التوقيع الرقمي عبر الانترنت (eSign).

تمكّن خدمة الثقة للتوقيع الرقمي مقدمي منصة التوقيع الرقمي (SIP) من دمج منصات الخدمة الرقمية الخاصة بهم مع مركز تصديق " إمضاء" للتوقيع الرقمي وبذلك يمكنهم تقديم خدمة التوقيع عن بُعد عبر الانترنت لتطبيقاتهم وعملائهم والمستخدمين النهائيين. وهي مسؤولة عن:

1. طلب واستلام معلومات العميل من الوكيل الموثوق لمعلومات العميل.
2. العمل كوسيط لمركز تصديق "إمضاء" للتوقيع الرقمي لاستلام ومعالجة معلومات العميل الخاصة بالعملاء.

2. Acting as a proxy for emdha eSign CA to receive and process subscriber KYC information;
3. Receiving and processing data-hash to securely perform subscriber signatures remotely;
4. Deleting the subscriber private keys at the end of every signature session;
5. Verifying and validating subscriber's digital signature request or/and related information received from authorized SIP,RKA and alike;
6. Securely retaining the evidence(s) for subscriber certificate issuance and digital signature creation;
7. Digitally signing response(s) to SIPs; and

Complying to any additional steps either regulatory or otherwise, deemed necessary to ensure or/and enhance the security of the eSign Trust Service.

1.4 Time-Stamp Authority (TSA)

TSA service provides an RFC 3161 compliant digitally-signed timestamp token whose signer vouches for the existence of the signed document, transaction or content at a certain point in time by recording their digitally signed fingerprint along with the date and time the transaction occurred. This service asserts that the data and/or associated secure hash existed at the specified time.

This service will be consumed by emdha's own eSign service for time-stamping transactions performed through the eSign service.

Time-stamping of transactions also allows for the transaction to be considered valid beyond the expiration of the subscriber certificate.
The TSA shall use a reliable time source whose clock is synchronized as per global best-practices. The TSA shall ensure time synchronization is performed at least once every 24 hours and ensure time drift is within 1 second of UTC time.

For the purpose of this Subscriber agreement, emdha eSign CA and TSA are considered to be a part of the eSign Trust Service.

1.5 Signing Interface Provider (SIP)

SIP is an organization or an entity using the eSign service(s) as part of their application to digitally sign the content. Examples include Government Departments, Banks and other public or private organizations. SIPs shall be responsible for:

1) Complying with and completing the necessary obligations stipulated by emdha eSign CA for on-boarding before they can start using the eSign Trust Service;
2) Securely communicating with eSign Trust Service using prescribed procedures mandated by emdha eSign CA.;
3) Receiving, validating and compiling transaction data/document(s) and ensuring that hash(es) are created for accurate and complete data prior to sending them to the eSign Trust Service;
4) Obtaining user-consent to permit eSign Trust Service to perform digital signature remotely;
5) Verifying and ensuring the digitally signed-hash(es) received from eSign Trust Service correspond to the respective

3. استلام ومعالجة هاش البيانات لتنفيذ توقيعات المشتركين عن بُعد بأمان.
4. حذف المفاتيح الخاصة بالمشترك عند نهاية كل عملية توقيع.
5. التحقق من صحة طلب التوقيع الرقمي الخاص بالمشترك والمعلومات المرتبطة بالتوقيع المستلمة من مقدم منصة واجهة التوقيع الرقمي SIP والوكيل الموثوق لمعلومات العميل الخ.
6. تأمين الاحتفاظ بالإثبات (الإثباتات) المتعلقة بإصدار شهادات المشترك وتنفيذ التوقيع الرقمي.
7. الرد/ الردود لمقدمي منصة التوقيع الرقمي (SIP) والتي تشتمل على التوقيع الرقمي.

الامتثال لأية خطوات إضافية (سواء كانت تنظيمية أو غير ذلك) تعتبر ضرورية لضمان أمان خدمة الثقة للتوقيع الرقمي.

4.1 مركز الختم الزمني TSA

يوفر مركز الختم الزمني توكن الختم الزمني المتزامن مع التوقيع الرقمي والملتزم بنظام RFC 3161 والذي يؤكد بموجبه وجود الوثيقة أو المعاملة أو المحتوى الموقع في فترة معينة من الوقت من خلال تسجيل بصمته الموقعة رقمياً الى جانب تاريخ ووقت المعاملة التي تمت. تؤكد هذه الخدمة ان البيانات و / او الهاش المرتبط بها قد وجدا في الوقت المحدد.

سوف يتم استخدام هذه الخدمة بواسطة خدمات "إمضاء" للتوقيع الرقمي بحيث يتم وضع الختم الزمني الى جانب التوقيع الرقمي.
أيضاً يسمح الختم الزمني للمعاملات بأن يتم اعتبارها سارية بعد انتهاء شهادة المشترك.

يستخدم مركز الختم الزمني مصدر موثوق لضبط التوقيت، حيث يتم ضبط الساعة وفقاً لأفضل الممارسات العالمية. سوف يضمن التوقيع الزمني أن مزامنة الوقت تتم كل 24 ساعة على الأقل كما يضمن أن لا يتجاوز الانحراف 1 ثانية بنظام التوقيت العالمي.

لغرض إتفاقية المشترك هذه، يعتبر كل من مركز تصديق "إمضاء" للتوقيع الرقمي ومركز الختم الزمني TSA جزءاً من خدمة الثقة للتوقيع الرقمي.

5.1 مقدم منصة واجهة التوقيع (SIP)

مقدم منصة واجهة التوقيع هو منشأة أو جهة تستخدم خدمات التوقيع الرقمي كجزء من تطبيقاتهم للتوقيع رقمياً على المحتوى. والامثلة لذلك تشمل الإدارات الحكومية والبنوك والمؤسسات العامة أو الخاصة الأخرى. يكون مقدم منصة واجهة التوقيع مسؤولاً عن:

1) إكمال والتقيد بالالتزامات الضرورية التي يشترطها مركز تصديق "إمضاء" للتوقيع الرقمي للتسجيل قبل بدء استخدام خدمة الثقة للتوقيع الرقمي.
2) التواصل بصورة آمنة مع خدمة الثقة للتوقيع الرقمي باستخدام الإجراءات المحددة المفروضة بواسطة مركز تصديق "إمضاء" للتوقيع الرقمي.
3) الاستلام والتحقق من وتجميع بيانات / وثيقة (وثائق) المعاملة وضمان أن الهاش قد تم إنشاؤه لبيانات دقيقة وكاملة قبل إرسالها الى خدمة التوقيع الرقمي.
4) الحصول على موافقة المستخدم على تمكين خدمة التوقيع الرقمي من تنفيذ التوقيع الرقمي عن بُعد.
5) التحقق وضمان أن بيانات الهاش الموقعة رقمياً المستلمة من خدمة الثقة للتوقيع الرقمي مطابقة لبيانات/ مستندات الهاش المرسل سلفاً من مقدم منصة واجهة

data/document(s) hash(es) sent earlier by the SIP;
6) Verifying and validating emdha eSign CA's digital signature(s) for every transaction received from eSign Trust Service;
7) Verifying and validating subscriber signature before relying on or processing the transaction;

SIP asserts that they use eSign Trust Services and processes associated with each transaction in accordance with the emdha eSign CA CP/CPS and this SIP/RKA Agreement.

1.6 Reliable KYC Agency (RKA)

RKA is an organization, other than BTC/emdha, listed in this document to act as a KYC (Know Your Customer) provider for the purpose of Online Signature Service (eSign Trust Service).

RKA is responsible for:

1) Subscriber's verification and authentication before providing the subscriber KYC information to emdha eSign CA. Such agency shall ensure the verification steps of the signatory shall be the same or higher than the verification steps required by emdha eSign CA to verify for issuance of Digital Signature Certificate;
2) Digitally signing subscriber KYC information using the prescribed certificate type before providing to the emdha eSign CA. It will be the basis for creation of the subscriber certificate;
3) Obtaining user-consent and perform at least a 2-factor authentication for each digital certificate/signature and key generation/request before providing the digitally-signed KYC information to emdha eSign CA or eSign trust service;
4) RKA asserts that they use eSign services and processes associated with each transaction in accordance with the emdha eSign CA CP/CPS and the RKA agreement.

Following are entities eligible to be RKA's under this policy:

1) Any establishment operating under the regulations of Saudi Central Bank (SAMA) in Kingdom of Saudi Arabia.
2) Absher or National IAM agency of the Kingdom of Saudi Arabia.
3) Ministry of Human Resources and Social Development
4) Any governmental establishment/institution that unconditionally relies only on Absher or National IAM agency for providing reliable KYC information of its end-user(s).
5) Any non-governmental establishment/institution that unconditionally relies only on Absher or National IAM agency for providing reliable KYC information of its end-user(s), and signs and submits a declaration that the signed KYC information received from Absher is shared with BTC with no modifications.

التوقيع.
6) فحص والتحقق من التوقيع الرقمي الصادر عن مركز تصديق "إمضاء" للتوقيع الرقمي لكل معاملة مستلمة من خدمة الثقة للتوقيع الرقمي.
7) فحص والتحقق من توقيع المشترك قبل الاعتماد عليه وانجاز المعاملة.

يؤكد مقدم منصة واجهة التوقيع أنه يستخدم خدمات التوقيع الرقمي والمعالجات المرتبطة بكل معاملة وفقاً لسياسات الشهادة الرقمية /إجراءات التصديق الرقمي (CP/CPS) الخاصة بمركز تصديق "إمضاء" للتوقيع الرقمي وإتفاقية مقدم منصة واجهة التوقيع والوكيل الموثوق لمعلومات العميل.

6.1 الوكيل الموثوق لمعلومات العميل (RKA)

الوكيل الموثوق لمعلومات العميل هي منشأة بخلاف شركة بُعد للاتصالات/ "إمضاء" ويشار اليها في هذه الوثيقة على انها تعمل كمقدم لمعلومات العملاء لغرض تنفيذ خدمة التوقيع عبر الانترنت (خدمة الثقة للتوقيع الرقمي).

الوكيل الموثوق لمعلومات العميل مسؤول عن:

1) التحقق والمصادقة على المشترك قبل توفير معلومات المشترك الى مركز تصديق "إمضاء" للتوقيع الرقمي. سوف تضمن هذه الجهة أن خطوات التحقق من الموقّع سوف تكون هي نفسها أو افضل من خطوات التحقق المطلوبة بواسطة مركز تصديق "إمضاء" للتوقيع الرقمي للتحقق من أجل إصدار شهادة التوقيع الرقمي.
2) توقيع معلومات العميل للمشترك رقمياً باستخدام نوعية الشهادة المحددة، وذلك قبل تقديمها لمركز تصديق "إمضاء" للتوقيع الرقمي، وسوف تكون الأساس لإنشاء شهادة المشترك.
3) الحصول على موافقة المستخدم وتنفيذ عملية التحقق ثنائي الحماية على الأقل لكل شهادة / توقيع رقمي وعملية إنتاج المفتاح/ طلب المفتاح قبل توفير معلومات العميل الموقعة رقمياً لمركز تصديق "إمضاء" للتوقيع الرقمي أو خدمة الثقة للتوقيع الرقمي.
4) يؤكد الوكيل الموثوق لمعلومات العميل أنه يستخدم خدمات التوقيع الرقمي والإجراءات المرتبطة بها في كل معاملة وفقاً لسياسات الشهادة الرقمية /إجراءات التصديق الرقمي (CP/CPS) الخاصة بـ مركز تصديق "إمضاء" للتوقيع الرقمي وإتفاقية الوكيل الموثوق لمعلومات العميل.

فيما يلي المنشآت/ الجهات المؤهلة لتعمل بصفتها الوكيل الموثوق لمعلومات العميل وتقديم معلومات العميل بموجب هذه السياسة:-

1) أي منشأة تعمل بموجب أنظمة البنك المركزي السعودي (مؤسسة النقد العربي السعودي ساما سابقاً) في المملكة العربية السعودية.
2) أبشر أو خدمة النفاذ الوطني الموحد (IAM) في المملكة العربية السعودية.
3) وزارة الموارد البشرية والتنمية الاجتماعية
4) أي منشأة / مؤسسة حكومية تعتمد بشكل غير مشروط على أبشر أو خدمة النفاذ الوطني الموحد (IAM) لتقديم معلومات العميل الموثوقة للمستخدم/ المستخدمين النهائيين.
5) أي منشأة / مؤسسة غير حكومية تعتمد دون قيد أو شرط على أبشر أو خدمة النفاذ الوطني الموحد (IAM) لتقديم معلومات العميل الموثوقة للمستخدم/ المستخدمين النهائيين، وتوقع وتقدم إقراراً بأن معلومات العميل الموقعة التي تم تلقيها من أبشر يتم تقديمها لشركة بُعد للاتصالات بدون تعديلات.

SIP and RKA are allowed to be the same organization, as long as both are authorized for each role.

يجوز أن يكون مقدم منصة واجهة التوقيع والوكيل الموثوق لمعلومات العميل هما نفس الجهة طالما أن كلاهما مفوض لأداء مثل هذه المهام.

1.7 Subscribers

Subscribers are individuals (end users/customers) or entities (organizations) to whom certificates are issued and are legally bound by a Subscriber Agreement or Terms of use.

7.1 المشتركون

المشتركون هم أفراد (مستخدمون نهائيون/ عملاء) او منشآت (أطراف) يتم إصدار الشهادات لهم وهم قانونياً مرتبطين بواسطة إتفاقية المشترك أو شروط الاستخدام.

1.8 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the CA's or subscriber's identity to a public key. The Relying Party is responsible for checking the validity of the certificate by examining the appropriate certificate status information, using validation services provided by the emdha eSign CA. A Relying Party's right to rely on a certificate issued under the emdha eSign CA CP/CPS, requirements for reliance, and limitations thereon, are governed by the terms of the emdha eSign CA CP/CPS and the Relying Party Agreement, that are available at www.emdha.sa.

8.1 الأطراف المُتعاملة

الطرف المُتعامل هو ذلك الجهة و/أو المنشأة التي تعتمد على صحة وصلاحية ارتباط سلطة التصديق أو هوية المشترك بالمفتاح العام. يكون الطرف المُتعامل مسؤولاً عن التحقق من صلاحية الشهادة من خلال فحص معلومات حالة الشهادة باستخدام خدمات التحقق الموفرة من قبل مركز تصديق "إمضاء" للتوقيع الرقمي. يكون للطرف المُتعامل الحق في الاعتماد على الشهادة الصادرة بموجب إجراءات التصديق الرقمي/ سياسات الشهادة الرقمية (CP/CPS) الخاصة بمركز تصديق "إمضاء" للتوقيع الرقمي واشتراطات وقيود التعامل والتي تخضع لشروط وإجراءات التصديق الرقمي/ سياسات الشهادة الرقمية (CP/CPS) الخاصة بمركز تصديق "إمضاء" للتوقيع الرقمي وإتفاقية الطرف المُتعامل والتي يمكن الحصول عليها بالدخول على الموقع www.emdha.sa.

Relying Parties shall use and rely on a certificate that has been issued under the emdha eSign CP/CPS if:

1) The certificate has been used for the purpose for which it has been issued, as described in the emdha eSign CA CP/CPS, and applicable Subscriber Agreement;
2) The Relying Party has verified the validity of the digital certificate, using procedures described in the Relying Party Agreement;
3) The Relying Party processes and understands certificate extensions in accordance with RFC 5280;
4) The Relying Party has accepted and agreed to the Relying Party Agreement at the time of relying on the certificate; it shall be deemed to have done so by relying on the certificate; and
5) The relying party accepts in totality, the certificate policy applicable to the certificate, which can be identified by reference of the certificate policy OID mentioned in the certificate.

سوف تستخدم الأطراف المُتعاملة وتعتمد على الشهادة التي تم إصدارها بموجب إجراءات التصديق الرقمي/ سياسات الشهادة الرقمية (CP/CPS) في الحالات التالية:

1) تم استخدام الشهادة للغرض الذي من أجله تم إصدارها حسبما هو محدد في سياسة مركز تصديق "إمضاء" للتوقيع الرقمي وإجراءات التصديق الرقمي/ سياسات الشهادة الرقمية (CP/CPS) وإتفاقية المشترك.
2) تحقق الطرف المُتعامل من سريان الشهادة الرقمية باستخدام الإجراءات المنصوص عليها في إتفاقية الطرف المُتعامل.
3) قام الطرف المُتعامل بمعالجة وفهم امتداد/ او محلق اسم الشهادة وفقاً لنظام RFC 5280،
4) قبل الطرف المُتعامل ووافق على إتفاقية الطرف المُتعامل عندما تم الاعتماد على الشهادة. وسوف يعتبر انه قد فعل ذلك عند الاعتماد على الشهادة، و
5) قبل الطرف المُتعامل إجمالاً سياسة الشهادة المطبقة عليها والتي يمكن تحديدها من خلال الرجوع إلى معرفّ السياسة (OID) المذكور في الشهادة.

1.9 Application Sponsor

Application Sponsor shall serve as the representative of an Application or Organization or SIP in order to register the application or organization or SIP and/or RKA with the eSign service and/or emdha eSign CA. Application Sponsor(s) shall be individual(s) authorized by the SIP and/or RKA to represent, act and contract on behalf of the SIP and/or RKA organization.

9.1 المسؤول عن التطبيق

يعمل المسؤول عن التطبيق كممثل للتطبيق أو لمنشأة أو مقدم منصة واجهة التوقيع من أجل تسجيل التطبيق أو المنشأة أو مقدم منصة واجهة التوقيع و / أو الوكيل الموثوق لمعلومات العميل في خدمة التوقيع الرقمي و / أو مركز تصديق "إمضاء" للتوقيع الرقمي. من الممكن ان يكون المسؤول عن التطبيق فرداً (أفراداً) مخولين بواسطة مقدم منصة واجهة التوقيع و / أو الوكيل الموثوق لمعلومات العميل لتمثيل والتصرف والتعاقد نيابة عن مقدم منصة واجهة التوقيع و / أو الوكيل الموثوق لمعلومات العميل.

1.10 Know Your Customer (KYC)

KYC means the transfer of digitally-signed demographic data such as Name, Address, Date of Birth, Gender, Mobile number, Email address, photograph, Customer Record Number, CRN, CIF, Citizen ID or Iqama ID, etc. of an individual, collected and verified by RKA on successful authentication of same individual.

10.1 معلومات العميل الموثوقة

يقصد بمعلومات العميل الموثوقة نقل البيانات الديموغرافية الموقعة رقمياً مثل الاسم والعنوان وتاريخ الميلاد ونوع الجنس ورقم الجوال وعنوان البريد الإلكتروني والصورة ورقم سجل العميل

1.11 BTC LICENSED CA

The term 'BTC LICENSED CA' refers to the CA entity owned and operated by BTC which is approved by DGA to join the Saudi National PKI, directly under the DGA root CA. 'emdha eSign CA' join directly under the BTC LICENSED CA.

2. Binding Agreement

Subscriber reads, agrees, represents and warrants to comply with the terms of this Subscriber Agreement ("Agreement") before applying for a certificate or associated signature(s) performed using certificates issued by emdha eSign CA.
Subscriber acknowledges and authorizes eSign Trust Service offered by BTC/emdha to centrally/remotely generate cryptographic keys and associated certificate on behalf of Subscriber, and may centrally/remotely perform digital signature on behalf of subscriber in accordance to the Subscriber Agreement and emdha eSign CA Certificate Policy (CP) / Certification Practices Statement (CPS).

Subscriber agrees that participation in this transaction will mean acceptance of this Agreement. Subscriber shall not participate in the transaction in case he/she/them do not wish to accept and agree to this Agreement.

The terms and conditions set forth herein (the "Agreement") constitute a final and binding agreement between the "Subscriber" and 'BTC Licensed CA' and/or 'emdha eSign CA' and/or eSign Trust Service with respect to any services related to the issuance and/or use of digital certificate issued on the subscriber's behalf by 'emdha eSign CA' and/or eSign Trust Service.

3. Subscriber Obligations

Subscriber is obligated to:

1) Attest to the truthfulness and accuracy of all information provided in the Application;
2) Accept and agree, in totality, to the terms and conditions of this Subscriber Agreement and the emdha eSign CA Certificate Policy (CP)/Certification Practices Statement (CPS);
3) Provide accurate and complete information at all times to the RKA;
4) Review and verify provided information for accuracy and completeness;
5) Secure authentication and consent mechanisms for certificate requests and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, Mobile Phone for OTP, or other activation data that is used to control access to the Subscriber's private key;
6) Subscriber is responsible to make all reasonable efforts to prevent the compromise, loss, disclosure, modification or otherwise unauthorized use of Subscriber resources from loss, theft, malware, virus, trojans, spyware, rootkits, etc.
7) Use Subscriber Certificate only for its intended use;

ورقم ملف معلومات العميل ورقم الهوية الوطنية ورقم الإقامة الخ للفرد حيث يتم جمعها والتحقق منها بواسطة الوكيل الموثوق لمعلومات العميل، وذلك بعد التحقق بنجاح عن هذا الفرد.

11.1 مركز تصديق بُعد المرخص

يشير مصطلح " مركز تصديق "بُعد" المرخص الى مركز التصديق الرقمي المملوك والمدار بواسطة شركة بُعد للاتصالات والذي هو معتمد من قبل هيئة الحكومة الرقمية بحيث ينضم الى البنية التحتية للمفاتيح العامة السعودية، ويعمل مباشرة تحت اشراف مركز التصديق الجذري السعودي والذي يتبع بدوره الى هيئة الحكومة الرقمية.

2. الإتفاقية الملزمة

يقرأ المشترك ويوافق ويتعهد ويضمن التقيد بشروط إتفاقية المشترك هذه ("الإتفاقية") قبل التقدم بطلب للحصول على شهادة أو توقيع (توقيعات) يتعلق بها يتم تنفيذه باستخدام الشهادات الصادرة بواسطة مركز تصديق "إمضاء" للتوقيع الرقمي.
يقر المشترك ويخول خدمة الثقة للتوقيع الرقمي التي تقدمها شركة بُعد للاتصالات / " إمضاء" بإصدار مفاتيح التشفير مركزياً وعن بُعد، وكذلك الشهادة المرتبطة بها نيابة عن المشترك، ويحق لها تنفيذ التوقيع الرقمي مركزياً عن بُعد نيابة عن المشترك وفقاً لإتفاقية المشترك وإجراءات التصديق الرقمي/ سياسات الشهادة الرقمية (CP/CPS) الخاصة بمركز تصديق "إمضاء" للتوقيع الرقمي.

يقر المشترك بأن المشاركة في هذه المعاملة سوف تعني قبول هذه الإتفاقية. يجب ألا يشارك المشترك في المعاملة في حالة أنه / أنها لا ترغب في قبول والموافقة على هذه الإتفاقية.

تشكل الشروط والأحكام المنصوص عليها في هذه الوثيقة ("الإتفاقية") إتفاقية ملزمة ونهائية بين "المشترك" ومركز تصديق "بُعد" المرخص و/ او مركز تصديق "إمضاء" للتوقيع الرقمي و/او خدمة الثقة للتوقيع الرقمي وذلك فيما يتعلق بأي خدمات تتعلق بإصدار و/ او استخدام الشهادات الرقمية الصادرة نيابة عن المشترك بواسطة مركز تصديق "إمضاء" للتوقيع الرقمي و/او خدمة الثقة للتوقيع الرقمي.

3. التزامات المشترك

يلتزم المشترك بالآتي:

1) يشهد بصحة ودقة كافة المعلومات المتوافرة في الطلب.
2) القبول والموافقة على جميع شروط وأحكام إتفاقية المشترك هذه وإجراءات التصديق الرقمي/ سياسات الشهادة الرقمية (CP/CPS) الخاصة بمركز تصديق "إمضاء" للتوقيع الرقمي.
3) توفير معلومات دقيقة وكاملة في كل الأوقات إلى الوكيل الموثوق لمعلومات العميل.
4) التدقيق والتحقق من صحة المعلومات المتوفرة لضمان الدقة والاكتمال.
5) تأمين وسائل وطرق التحقق من الصحة والموافقات الخاصة بطلبات الشهادات واتخاذ الاحتياطات المعقولة والضرورية لمنع فقدان أو كشف أو تعديل أو الاستخدام غير المخول للمفاتيح الخاصة. ويشمل هذا كلمة السر وجهاز التوكن والجوال لـكلمة السر لمرة واحدة"OTP" أو البيانات الأخرى المستخدمة للتحكم في إمكانية الدخول إلى المفاتيح الخاصة للمشترك.
6) يكون المشترك مسؤولاً عن بذل قصارى جهده للمحافظة على موارده ومعلوماته الخاصة والحيلولة دونها والاختراق والفقدان او الانكشاف او التعديل او تصرف آخر

غير مصرح به مما قد يعرضها للسرقة او الفقدان او البرامج الضارة او الفيروسات وبرامج التجسس والاختراق بأنواعها المختلفة (trojans, spyware, rootkits) .

7) استخدام شهادة المشترك فقط للغرض المطلوب.

8) إخطار الوكيل الموثوق لمعلومات العميل ومقدم منصة واجهة التوقيع في حالة ان أي معلومات في الشهادة كانت او اصبحت غير صحيحة او غير دقيقة.

9) إخطار مركز التصديق / مقدم منصة واجهة التوقيع فوراً في حالة تعرض مفتاح للخطر او عندما يتوفر للمشترك سبب يدعو للاعتقاد بأن المفتاح الخاص بالمشترك قد تم الدخول إليه بواسطة فرد آخر أو تم اختراقه بأي طريقة ما.

10) استخدام شهادة المشترك بطريقة لا تنتهك الأنظمة المعمول بها في المملكة العربية السعودية، و

11) عند إنهاء إتفاقية المشترك، إخطار مقدم منصة واجهة التوقيع فوراً لإيقاف استخدام شهادة المشترك.

12) يقبل المشترك بمركز تصديق "إمضاء" للتوقيع الرقمي ومركز تصديق "بُعد" المرخص وخدمات الثقة للتوقيع الرقمي المقدمة من " إمضاء" / شركة بُعد للاتصالات كأنظمة موثوقة.

13) يقبل المشترك ويوافق ويخول خدمة الثقة للتوقيع الرقمي لإصدار مفاتيح مشفرة مركزياً/ عن بُعد نيابة عن المستخدم واستخدام هذه المفاتيح لطلب الشهادات المرتبطة بهوية المشترك ولطلب واصدار التوقيعات نيابة عن المشترك. يوافق المشترك بأن أي استخدام لمفاتيح المشترك هذه و / أو الشهادة لتوقيع أو اعتماد محتويات أي سجل أو رسالة إلكترونية، انما هو امر يعود للمشترك. يوافق المشترك على الالتزام قانونياً بمحتويات أي سجل أو رسالة إلكترونية.

4. الضمان

بموجبه ينفي مركز تصديق "بُعد" المرخص و/أو "مركز تصديق " إمضاء" للتوقيع الرقمي المسؤولية عن اي ضمانات ويشمل ذلك ضمان قابلية التسويق و/أو الملائمة لغرض معين بخلاف ذلك المحظور بواسطة النظام أو بخلاف ما تم تقديمه بنص صريح ضمن إجراءات التصديق الرقمي/ سياسات الشهادة الرقمية (CP/CPS) الخاصة بمركز تصديق "إمضاء" للتوقيع الرقمي/ مركز تصديق "بُعد" المرخص.

تسعى كل من مركز تصديق "بُعد" المرخص و/ أو مركز تصديق "إمضاء" للتوقيع الرقمي عبر المكونات ذات الصلة لتوفير خدمات تصديق رقمي وفقاً للمعايير العالمية وأفضل الممارسات باستخدام افضل التجهيزات المادية والإلكترونية.

لا يقدم مركز تصديق "بُعد" المرخص و/ أو مركز تصديق "إمضاء" للتوقيع الرقمي أي ضمان صريح أو ضمني أو قانوني أو بأي شكل آخر ويعلنان عدم المسؤولية عن نجاح أو إخفاق مركز تصديق "بُعد" المرخص و/ أو مركز تصديق "إمضاء" للتوقيع الرقمي أو عن السريان القانوني أو قبول أو أي نوع آخر من الاعتراف بشهاداته أو أي توقيع رقمي يتم بموجب هذه الشهادات أو أي منتجات/ حلول/ خدمات موفرة بواسطة مركز تصديق "بُعد" المرخص و/ أو " مركز تصديق "إمضاء" للتوقيع الرقمي. أيضاً يعلن كل من " مركز تصديق "بُعد" المرخص و/ أو " مركز تصديق "إمضاء" للتوقيع الرقمي عدم المسؤولية عن أي ضمان يتعلق بقابلية التسويق و / أو الملاءمة لغرض معين للشهادات الصادرة والتوقيعات الرقمية والمنتجات/ الحلول/ الخدمات.

يتم تقديم الخدمات الموفرة بواسطة خدمة الثقة للتوقيع الرقمي للمشتركين كما هي وعلى أساس ما هو متاح. وتعلن خدمة الثقة للتوقيع الرقمي بشكل صريح عدم المسؤولية عن كافة الضمانات الأخرى المرتبطة بأي شهادة مشترك أو أي خدمات مرتبطة موفرة بواسطة خدمة الثقة للتوقيع الرقمي، ويشمل ذلك ولكن ليس حصراً على أي ضمان بعدم انتهاك أو قابلية

8) Notify the RKA and SIP in the event of any information in the Certificate is, or becomes, incorrect or inaccurate;

9) Notify the CA/SIP in the event of a key compromise immediately whenever the Subscriber has reason to believe that the Subscriber's private key has been accessed by another individual, or compromised in any other manner;

10) Use the Subscriber Certificate in a manner that does not violate applicable laws in the Kingdom of Saudi Arabia; and

11) Upon termination of Subscriber Agreement, immediately notify the SIP to cease use of the Subscriber Certificate.

12) Subscriber accepts 'emdha eSign CA' and 'BTC Licensed CA' and 'eSign Trust Service' provided by Baud Telecom Company (BTC) / emdha as trustworthy systems;

13) Subscriber accepts, consents, agrees and authorizes eSign Trust Service to centrally/remotely generate cryptographic keys on behalf of the user and use such keys to request for associated certificates bound to the subscriber identity and for requesting and generating signatures on behalf of the Subscriber. Subscriber agrees that any use of such Subscriber keys and/or certificate to sign or otherwise approve the contents of any electronic record or message is attributable to Subscriber. Subscriber agrees to be legally bound by the contents of any such electronic record or message.

4. Warranty

'BTC Licensed CA' and/or 'emdha eSign CA' hereby disclaims all warranties including warranty on merchantability and /or fitness to a particular purpose other than to the extent prohibited by law or otherwise expressly provided in 'BTC Licensed CA' and/or 'emdha eSign CA' CP/CPS.

'BTC Licensed CA' and/or 'emdha eSign CA', through its associated components, seeks to provide digital certification services according to international standards and best practices, using secure physical and electronic installations.

'BTC Licensed CA' and/or 'emdha eSign CA' provides no warranty, express, or implied, statutory or otherwise and disclaims any and all liability for the success or failure of the deployment of the 'BTC Licensed CA' and/or 'emdha eSign CA' or for the legal validity, acceptance or any other type of recognition of its own certificates, any digital signature backed by such certificates, and any products/solutions/services provided by 'BTC Licensed CA' and/or 'emdha eSign CA'. 'BTC Licensed CA' and/or 'emdha eSign CA' further disclaims any warranty of merchantability or fitness for a particular purpose of the issued certificates, digital signatures and products/solutions/services.

Services provided by eSign Trust Service to Subscribers are provided on an "As is" and "As available" basis, and eSign Trust Service expressly disclaims all other warranties relating to any Subscriber Certificate or any related services provided by eSign Trust Service including, but not limited to, any warranty of no infringement, merchantability, or fitness for a particular purpose. eSign Trust Service does not warrant that their certificates will be compatible of functional with any software. Furthermore, you are hereby notified of the possibility of compromise of a private key corresponding to a public

key contained in a Subscriber Certificate, including theft, which may or may not be detected, and of the possibility of use of a stolen or compromised key to forge a digital signature to a document.

التسويق أو الملاءمة لغرض معين. لا تضمن خدمة الثقة للتوقيع الرقمي أن شهاداتها سوف تكون متوافقة وظيفياً مع أي برمجيات. علاوة على ذلك، يتم إخطاركم باحتمالية ان يتعرض للخطر المفتاح الخاص المطابق لمفتاح عام والموجود في شهادة المشترك ويشمل ذلك السرقة والتي يمكن أو لا يمكن كشفها واحتمالية استخدام المفتاح المسروق أو المخترق لتزوير التوقيع الرقمي على وثيقة.

5. Indemnity and Limitation of Liability

5. التعويض وحدود المسؤولية

This section applies to liability under contract (including breach of warranty), tort (including negligence and/or strict liability), and any other legal or equitable form of claim.

ينطبق هذا القسم على المسؤولية بموجب العقد (ويشمل الإخلال بالضمان)، والمسئولية التقصيرية (ويشمل الإهمال و/ أو المسؤولية المشددة) وأي نوع آخر من المطالبات القانونية أو التي تطالب بالإنصاف.

‘eSign Trust Service’ and/or ‘BTC Licensed CA’ and/or ‘emdha eSign CA’ disclaims liability to the certificate beneficiaries or Subscriber or relying parties or any other third-parties for any loss suffered as a result of use or reliance on a certificate beyond those specified in ‘BTC Licensed CA’ and/or ‘emdha eSign CA’ CP/CPS, when such certificate has been issued and managed by ‘eSign Trust Service’ and/or ‘BTC Licensed CA’ and/or ‘emdha eSign CA’ in compliance with said CP/CPS. In any other case:

إن خدمة الثقة للتوقيع الرقمي و / أو مركز تصديق "بُعد" المرخص و/ أو مركز تصديق "إمضاء" للتوقيع الرقمي يخلون مسؤوليتهم تجاه أي مستفيدين من الشهادة أو المشتركين أو الأطراف المُتعاملة أو أي أطراف أخرى عن أي خسارة متكبدة نتيجة لاستخدام الشهادة أو الاعتماد عليها بخلاف تلك المحددة في إجراءات التصديق الرقمي/ سياسات الشهادة الرقمية(CP/CPS) الخاصة بمركز تصديق "بُعد" المرخص و/ أو مركز تصديق "إمضاء" للتوقيع الرقمي عندما يتم إصدار هذه الشهادات وإدارتها بواسطة خدمة الثقة للتوقيع الرقمي و / أو مركز تصديق "بُعد" المرخص و/ أو مركز تصديق "إمضاء" للتوقيع الرقمي وفقاً إجراءات التصديق الرقمي/ سياسات الشهادة الرقمية(CP/CPS). وفي جميع الأحوال الأخرى:

1) ‘eSign Trust Service’ will not incur any liability to Subscriber or relying parties or any person to the extent that such liability results from their negligence, fraud or willful misconduct;
1) لا تتحمل خدمة الثقة للتوقيع الرقمي أي مسؤولية تجاه المشترك أو الأطراف المُتعاملة أو أي شخص طالما ان هذه المسؤولية ناتجة عن إهمال أو غش أو سوء تصرف متعمد من قبل ذلك الطرف.

2) ‘eSign Trust Service’ assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued for any use other than in accordance with ‘BTC Licensed CA’ and/or ‘emdha eSign CA’ CP/CPS. Subscriber shall immediately indemnify ‘eSign Trust Service’ from and against any such liability and costs and claims arising therefrom;
2) لا تتحمل خدمة الثقة للتوقيع الرقمي أي مسؤولية مهما كانت فيما يتعلق باستخدام الشهادات أو ما يتعلق بها من أزواج المفاتيح العامة/المفاتيح الخاصة الصادرة لأي استخدام بخلاف ما هو محدد وفقاً في إجراءات التصديق الرقمي/ سياسات الشهادة الرقمية (CP/CPS) الخاصة بمركز تصديق "بُعد" المرخص و/ أو مركز تصديق "إمضاء" للتوقيع الرقمي. يجب على المشترك فوراً تعويض خدمة الثقة للتوقيع الرقمي عن ومقابل أي مسؤولية وتكاليف ودعاوى تنشأ عن ذلك.

3) ‘eSign Trust Service’ will not be liable to any party whosoever for any damages suffered whether directly or indirectly as a result of an uncontrollable disruption of its services;
3) لن تكون خدمة الثقة للتوقيع الرقمي مسؤولة أمام أي طرف مهما يكن عن أي أضرار متكبدة سواء بطريقة مباشرة أو غير مباشرة نتيجة لانقطاع خدماتها نتيجة لسبب خارج عن السيطرة.

4) End-Users / Subscribers are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been accepted by ‘eSign Trust Service’;
4) يكون المستخدمون النهائيون/المشتركون مسؤولون تجاه الأطراف المُتعاملة عن أي شكل من أشكال تحريف للمعلومات المضمنة في الشهادة حتى لو تم قبول المعلومات بواسطة خدمة الثقة للتوقيع الرقمي.

5) Subscribers to compensate a Relying Party which incurs a loss as a result of the Subscriber’s breach of Subscriber agreement;
5) يعوض المشتركون الطرف المُتعامل عن الخسارة المتكبدة نتيجة لانتهاك المشترك لإتفاقية المشترك.

6) Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations;
6) سوف تتحمل الأطراف المُتعاملة عواقب اخفاقها في تنفيذ التزامات الطرف المُتعامل.

7) RKAs shall bear the consequences of their failure to perform the obligations described in the RKA agreement;
7) سوف يتحمل الوكيل الموثوق لمعلومات العميل عواقب الاخفاق في تنفيذ التزاماته المنصوص عليها في إتفاقية الوكيل الموثوق لمعلومات العميل.

8) ‘eSign Trust Service’ denies any financial or any other kind of responsibility for damages or impairments resulting from its eSign Trust Service or CA operations;
8) تنفي خدمة الثقة للتوقيع الرقمي أي مسؤولية مالية أو أي نوع آخر من المسؤولية عن الأضرار أو المشاكل الناتجة عن خدماتها أو عمليات التصديق الرقمي.

9) Subscriber shall indemnify and hold emdha eSign CA and eSign Trust Service harmless from and against any and all damages (including legal fees), losses, lawsuits, claims or actions arising out of:
9) سوف يعوض المشترك ويحمي مركز تصديق "إمضاء" للتوقيع الرقمي وخدمة الثقة للتوقيع الرقمي عن كافة الأضرار (وتشمل الرسوم القانونية) أو الخسائر أو القضايا أو الدعاوى أو الأفعال الناتجة عن:

   1) Use of Subscriber’s Certificate in a manner not authorized by the CA/SIP or otherwise inconsistent with the terms of the Subscriber Agreement or the emdha eSign CA Certificate Policy (CP)/Certification Practices Statement (CPS);
   1) استخدام شهادة المشترك بطريقة غير تلك المحددة بواسطة مركز التصديق / مقدم منصة واجهة التوقيع SIP أو بطريقة ما لا تتفق مع شروط إتفاقية المشترك

   2) A Subscriber Certificate being tampered with by the Subscriber; or

3) Inaccuracies or misrepresentations contained within the RKA records for the subscriber.

A Subscriber shall indemnify and hold the emdha eSign CA and eSign Trust Service harmless against any damages and legal fees that arise out of lawsuits, claims or actions by third parties who rely on or otherwise use Subscriber's Certificate, where such lawsuit, claim, or action relates to a Subscriber's breach of its obligations outlined in this Subscriber Agreement or the emdha eSign CA CP/CPS, a Subscriber's failure to protect its authentication material or devices, or claims pertaining to content or other information or data supplied, or required to be supplied, by Subscriber.

أو إجراءات التصديق الرقمي/ سياسات الشهادة الرقمية (CP/CPS) الصادرة عن مركز تصديق "إمضاء" للتوقيع الرقمي.

2) العبث بشهادة المشترك من قبل المشترك.

3) البيانات الغير صحيحة او غير دقيقة المدرجة في سجلات الوكيل الموثوق لمعلومات العميل.

سوف يعوض المشترك ويحمي مركز تصديق "إمضاء" للتوقيع الرقمي عن كافة الأضرار والرسوم القانونية التي تنشأ نتيجة القضايا أو الدعاوى أو الإجراءات بواسطة أطراف ثالثة تعتمد على أو تستخدم شهادة المشترك بطريقة ما وذلك عندما تتعلق هذه القضية أو الدعوى أو الإجراء بانتهاك المشترك لالتزاماته المحددة في إتفاقية المشترك و إجراءات التصديق الرقمي/ سياسات الشهادة الرقمية(CP/CPS) الخاصة بمركز تصديق "إمضاء" للتوقيع الرقمي أو اخفق المشترك في حماية انظمة أو أجهزة التحقق من الصحة الخاصة به أو في حالة الدعاوى المتعلقة بالمحتوى أو المعلومات أو البيانات الموفرة أو المطلوب توفيرها بواسطة المشترك.

6. Use of Personal Information

6. استخدام المعلومات الشخصية

Subscriber hereby authorizes eSign Trust Service and emdha eSign CA to store all subscriber information submitted by the Subscriber/SIP/RKA as part of the Application, and to release that information, or some portion of that information, to a Relying Party upon the successful validation of Subscriber's Certificate by that Relying Party. eSign Trust Service or emdha eSign CA shall not disclose information related to the Subscriber, except under the terms and conditions set forth in the emdha eSign CA CP / CPS, Privacy policy, and otherwise as required by law. Each Relying Party is obligated to enter into a Relying Party Agreement with eSign Trust Service that limits the purposes for which a Relying Party may use or disclose information obtained, to those purposes that are authorized by the emdha eSign CA CP / CPS, subject to the conditions and limitations set forth therein. eSign Trust Service and Relying Parties must endeavor to:

(1) Ensure the confidentiality of personal data and business records;
(2) Prevent the sale or transfer of the personal data and business records; and
(3) Prevent the examination of or tampering with personal data or business records other than for the purposes of maintenance or security of the relevant information processing system or data integrity.

يخول المشترك خدمة الثقة للتوقيع الرقمي ومركز تصديق "إمضاء" للتوقيع الرقمي لتخزين كافة المعلومات المقدمة بواسطة المشترك/ مقدم منصة واجهة التوقيع/ الوكيل الموثوق لمعلومات العميل كجزء من التطبيق وتقديم تلك المعلومات أو جزء من تلك المعلومات إلى الطرف المُتعامل عند التحقق الناجح من شهادة المشترك بواسطة الطرف المُتعامل. لن تكشف خدمة الثقة للتوقيع الرقمي أو مركز تصديق "إمضاء" للتوقيع الرقمي المعلومات المتعلقة بالمشترك باستثناء ماهو منصوص عليه في إجراءات التصديق الرقمي/ سياسات الشهادة الرقمية (CP/CPS) وسياسة الخصوصية وفيما عدا ذلك وفقاً لما هو مطلوب بواسطة النظام. يكون كل طرف مُتعامل ملزماً بالدخول في إتفاقية الطرف المُتعامل مع خدمة الثقة للتوقيع الرقمي والتي تحدد الأغراض التي من أجلها يحق للطرف المُتعامل استخدام أو الكشف عن المعلومات التي حصل عليها بما يقتصر فقط على تلك الأغراض الموضحة في إجراءات التصديق الرقمي/ سياسات الشهادة الرقمية (CP/CPS) الخاصة بمركز تصديق "إمضاء" للتوقيع الرقمي ، وبما يخضع للشروط والقيود المنصوص عليها في هذه الوثيقة. ويجب على كل من خدمة الثقة للتوقيع الرقمي والأطراف المُتعاملة السعي لتحقيق الآتي:

(1) ضمان سرية البيانات الشخصية وسجلات العمل
(2) منع بيع أو نقل البيانات الشخصية أو سجلات العمل، و
(3) منع فحص أو العبث بالبيانات الشخصية أو سجلات العمل لأي غرض بخلاف أغراض محددة وهي: تأمين أو أمن نظام معالجة المعلومات او سلامة البيانات.

7. Term

7. المدة

This Subscriber Agreement is effective upon acceptance of transaction by subscriber and will terminate on the expiration date of the Subscriber Certificate(s) issued under this Subscriber Agreement or the expiry of the Time-Stamp Token applied to the signature transaction, whichever is later.

تكون إتفاقية المشترك هذه سارية المفعول عند قبول المعاملة بواسطة المشترك وسوف تنتهي عند تاريخ انتهاء شهادة (شهادات) المشترك الصادرة بموجب إتفاقية المشترك هذه أو انتهاء توكن الختم الزمني المطبق على معاملة التوقيع أيهما يأتي لاحقاً.

8. Assignment

8. التنازل

Subscriber shall not assign its rights or delegate its obligations under

لا يحق للمشترك التنازل عن حقوقه أو تفويض التزاماته بموجب إتفاقية المشترك هذه إلى أي طرف ثالث.

this Subscriber Agreement to any third party.

9. Termination

Subscriber shall not terminate the transaction with the eSign Trust Service or emdha eSign CA. Requirement(s) to terminate the transaction shall only be affected by informing the SIP through which the transaction was performed.

10. Entire Agreement

This Agreement with all documents referred to herein shall constitute the entire agreement between the Subscriber and 'emdha eSign CA' with respect to the Subscriber's request, use and acceptance of Subscriber keys and certificate. This Agreement shall supersede any other existing agreements between the Subscriber and 'emdha eSign CA', whether oral or written, with respect to the subject matter hereof.

11. Amendment and Waiver

eSign Trust Service reserves the right to amend this Agreement and the 'BTC Licensed CA' and/or 'emdha eSign CA' CP/CPS at any time without prior notice. All such amendments shall be made by posting the amended CP/CPS or the amended Agreement to https://www.emdha.sa. Any such amendment shall be effective as of the date of posting to https://www.emdha.sa.

A waiver of any provision of this Agreement must be in writing, designated as such, and signed by the party against whom enforcement of that waiver is sought. The waiver by a party of a breach of any provision of this Agreement shall not operate or be construed as a waiver of any subsequent or other breach thereof.

12. Governing Law

This Subscriber Agreement shall be governed and construed in accordance with the laws of Saudi Arabia.

13. Fiduciary Relationship

'eSign Trust Service' and/or 'BTC Licensed CA' and/or 'emdha eSign CA' is/are not the agent, fiduciary, trustee, or other representative of the Subscriber. Subscriber does not have any authority to bind 'eSign Trust Service' and/or 'BTC Licensed CA' and/or 'emdha eSign CA' by contract or otherwise, to any obligation. Subscriber shall make no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

14. Severability

Should any provision, or portion of any provision, of this Agreement be invalid or unenforceable for any reason, the validity or enforceability of the remaining provisions, or of the other portions of the provision in question shall not be affected thereby; provided, that such severance shall have no material adverse effect on the terms of this Agreement, and this Agreement shall be carried out as if any such invalid or unenforceable provision or portion of any provision were not contained herein.

9. الفسخ

لا يحق للمشترك إنهاء المعاملة مع خدمة الثقة للتوقيع الرقمي أو مركز تصديق "إمضاء" للتوقيع الرقمي. عند الرغبة في إنهاء المعاملة يتم ذلك فقط من خلال إبلاغ مقدم منصة واجهة التوقيع الذي يتم عبره تنفيذ المعاملة.

10. كامل الإتفاقية

تشكل هذه الإتفاقية مع كافة الوثائق المشار إليها بهذه الوثيقة مجمل الاتفاق بين المشترك و مركز تصديق "إمضاء" للتوقيع الرقمي فيما يتعلق بطلب المشترك واستعمال وقبول مفاتيح وشهادة المشترك. تلغي هذه الإتفاقية أي اتفاقيات أخرى قائمة بين المشترك ومركز تصديق "إمضاء" للتوقيع الرقمي، سواء كانت شفهياً أو كتابة فيما يتعلق بموضوعها.

11. التعديل والتنازل

تحتفظ خدمة الثقة للتوقيع الرقمي بحق تعديل هذه الإتفاقية وايضاً تعديل إجراءات التصديق الرقمي/ سياسات الشهادة الرقمية (CP/CPS) الخاصة بمركز تصديق "بُعد" المرخص ومركز تصديق "إمضاء" للتوقيع الرقمي في أي وقت بدون إشعار مسبق. تتم كافة هذه التعديلات عن طريق نشر إجراءات التصديق الرقمي/ سياسات الشهادة الرقمية (CP/CPS) المعدلة أو الإتفاقية المعدلة في الموقع https://www.emdha.sa. سوف يكون أي تعديل نافذاً ابتداء من تاريخ النشر في الموقع: https://www.emdha.sa.

يجب أن يكون أي تنازل عن أي بنود هذه الإتفاقية كتابة ومحدد بتلك الصفة وموقع بواسطة الطرف الذي سوف يطبق تجاهه هذا التنازل. التنازل الذي يتم بواسطة أي طرف ويتضمن الإخلال بأي فقرة بهذه الإتفاقية لن يكون نافذاً ولن يتم تفسيره كتنازل عند حدوث أي خرق لاحق.

12. النظام المعمول به

تخضع إتفاقية المشترك هذه وتفسر وفقاً للأنظمة المطبقة في المملكة العربية السعودية.

13. العلاقة الائتمانية

لا يعتبر أي من خدمة الثقة للتوقيع الرقمي و/أو مركز تصديق "بُعد" المرخص ومركز تصديق "إمضاء" للتوقيع الرقمي وكيلاً أو مؤتمناً أو وصياً أو ممثلاً للمشترك. ولا يملك المشترك أي سلطة لإلزام خدمة الثقة للتوقيع الرقمي و/أو " مركز تصديق "بُعد" المرخص ومركز تصديق "إمضاء" للتوقيع الرقمي بموجب عقد أو خلافاً لذلك بأي التزام. لن يقدم المشترك أي تعهدات خلافاً لذلك سواء بصورة صريحة أو ضمنية أو بالحضور أو خلاف ذلك.

14. قابلية التجزئة

إذا ما أصبحت أي فقرة أو جزء من فقرة بهذه الإتفاقية غير صالح أو غير قابل للتنفيذ لأي سبب، فإن صلاحية أو قابلية إنفاذ الفقرات المتبقية او الأقسام الأخرى لن تتأثر بذلك، بشرط أن شرط قابلية التجزئة هذا لن يؤثر جوهرياً بشكل سلبي على شروط هذه الإتفاقية، وسيتم تنفيذ هذه الإتفاقية كما لو أن الفقرة او الجزء من الفقرة الغير قابلة للتطبيق أو غير القابل للإنفاذ لم يتم تضمينها في هذه الوثيقة

15. تسوية النزاعات

15. Dispute Resolution

Any controversy or claim arising out of or relating to this Agreement shall be dealt with in accordance with the 'BTC PKI Complaint and Dispute Resolution Policy' and is roughly outlined as follows:

15.1 Negotiation: BTC/emdha will use its best efforts to resolve a complaint or dispute to the mutual satisfaction of the related parties and the complainant;

15.2 If both parties have not reached a solution in the agreed time frame, each party may give a written notice for Independent Mediation to resolve the dispute;

15.3 If mediation is not successful, then the dispute will be submitted to the competent courts of Riyadh, Saudi Arabia.

15.4 For government entities, the Independent Mediation is optional, and the dispute can be submitted to the competent courts of Riyadh, Saudi Arabia, if negotiations fail.

Subscriber agrees that any controversy, claim or dispute resolution proceedings will be conducted only on an individual basis and not in a class, consolidated, or representative action.

16. Force Majeure

No party shall be liable for any failure to perform its obligations in connection with any communication or transaction, where such failure results from any act of God, compliance with any law, regulation, order or legal process to which such party is subject, or other cause beyond such party's reasonable control (including, without limitation, any mechanical, electronic or communications failure) which prevents such Party from communicating under the terms of this agreement.

16. Survival

The following provisions in this agreement shall survive termination or expiration of this Agreement for any reason: (Limitation of Liability), (Term), (Assignment), (Termination), (Governing Law), (Fiduciary Relationship), (Severability), (Dispute Resolution) and (Survival).

17. Notices

All notices, questions, and requests shall be in English and shall be sent by email transmission to policy@emdha.sa. Notices to Relying Parties shall be made by posting the notice on the Repository https://www.emdha.sa and shall be deemed to be served upon the time of posting.

18. Prevailing Language

If this version of the Agreement exists in any other language(s), the English language version of this Agreement shall prevail, in case of any conflict between the English version and the other language versions.

*****End of eSign Subscriber Agreement******

يتم التعامل مع أي خلاف أو مطالبة تنشأ عن هذه الإتفاقية أو تتعلق بها وفقًا لـ"سياسة الشكاوى وحل النزاعات الخاصة بـ شركة بُعد للاتصالات فيما يتعلق بالبنية التحتية للمفاتيح العامة، والموضحة عموماً ادناه:-

15.1 التفاوض: ستبذل "إمضاء" /شركة بُعد للاتصالات قصارى جهدهما لحل الشكوى أو النزاع بما يرضي الأطراف ذات الصلة والمشتكي.

15.2 إذا لم يتوصل الطرفان إلى حل خلال الفترة المتفق عليها، يجوز لأي من الطرف تقديم إشعار كتابي لإحالة النزاع للوسيط المستقل للتوصل الى حل.

15.3 إذا لم تنجح الوساطة، فسيتم رفع النزاع إلى المحاكم المختصة في الرياض، المملكة العربية السعودية.

15.4 بالنسبة للجهات الحكومية، تعتبر الوساطة المستقلة اختيارية، ويمكن إحالة النزاع إلى المحاكم المختصة في الرياض، المملكة العربية السعودية إذا اخفقت المفاوضات.

يوافق المشترك على أن أي خلاف أو مطالبة أو إجراءات لتسوية النزاع سيتم إجراؤها فقط على أساس فردي وليس في إجراء جماعي أو موحد أو تمثيلي.

16. القوة القاهرة

لن يكون أي طرف مسؤولاً عن أي اخفاق في تنفيذ التزاماته فيما يتعلق بأي اتصال أو معاملة عندما يكون هذا الاخفاق نتيجة للقضاء والقدر أو الالتزام بأي نظام أو لوائح أو أمر أو إجراء قانوني يخضع له هذا الطرف أو سبب آخر خارج السيطرة المعقولة لذلك الطرف (ويشمل ذلك، على سبيل المثال وليس الحصر، أي عطل ميكانيكي أو الكتروني أو في الاتصالات) يمنع هذا الطرف من التواصل بموجب شروط هذه الإتفاقية.

16. السريان بعد الفسخ

تسري الأحكام التالية في هذه الإتفاقية بعد إنهاء أو انتهاء هذه الإتفاقية لأي سبب من الأسباب: (حدود المسؤولية) و (المدة) و (التنازل) و (الفسخ) و (النظام المعمول به) و (العلاقة الائتمانية) و (قابلية التجزئة) و (تسوية النزاعات) و (السريان بعد الفسخ).

17. الإشعارات

كافة الإشعارات والاستفسارات والطلبات تكون باللغة الإنجليزية ويتم إرسالها بواسطة البريد الإلكتروني إلى : policy@emdha.sa. ترسل الإشعارات إلى الأطراف المُتعاملة عن طريق وضع الإشعار في الموقع: https://www.emdha.sa وتعتبر قد تم تقديمها حينما يتم وضعها في الموقع.

18. اللغة السائدة

حررت هذه الإتفاقية باللغتين العربية والانجليزية، حيث إن النص الانجليزي يسود في حالة أي اختلاف بين النصين أو تفسير أي منهما.

**** نهاية إتفاقية المشترك في خدمة التوقيع الرقمي*****