TRUSTID® | IDENTRUST TLS/SSL | ORGANIZATION IDENTITY | ORGANIZATION VALIDATED (OV) CERTIFICATE SUBSCRIBER AGREEMENT

Clicking through the enrollment process (or downloading, installing, or using the Server Certificate) shall for all legal purposes constitute Subscriber's "signed" acceptance of the terms and conditions of this Agreement. If Subscriber does not agree to all of the terms of this Agreement, then do not proceed any further through the enrollment process.

1. Definitions. Unless otherwise defined herein, capitalized terms used herein shall have the meanings ascribed to them in Section 19 of this Agreement.

2. Scope. This Agreement establishes Subscriber's rights, duties and obligations as the Applicant for one or more TrustID Certificate and, if issued by IdenTrust pursuant in response to such application, one or more Server Certificates.

3. TrustID Certificate Issuance.

3.1. Application. The contents of the Server Certificate requested will be based on the information entered on the previous screens as part of the completed registration and application forms. The Individual completing the registration and agreeing to this Agreement represents and warrants that they have full power and authority to enter into this Agreement on behalf of Subscriber and that Subscriber will thereby be fully bound by the terms of this Agreement. By entering into this Agreement, Subscriber represents and warrants that: (i) all of the information submitted to IdenTrust (including without limitation Organization names and domain names) is accurate, current, complete, and not misleading; (ii) Subscriber owns the right to use such Organization and domain names; and (iii) Subscriber has provided all facts material to confirming its identity and to establishing the reliability of the information Subscriber has provided to IdenTrust for incorporation into a Server Certificate by IdenTrust pursuant to this Agreement. Subscriber agrees to provide such further information as IdenTrust may reasonably require in connection with the application and the Identification and Authentication process.

3.2. Key Pair Generation. Subscriber shall generate a Key Pair (Public and Private Keys) and submit the Public Key of such Key Pair with Subscriber's application. When IdenTrust creates the Server Certificate to be, the Public Key submitted with the application will be included in such Server Certificate. IN NO EVENT WILL IDENTRUST EVER HAVE ACCESS TO THE PRIVATE KEY OF THE KEY PAIR GENERATED BY SUBSCRIBER.

3.3. Verification of Identity and Authorization. Subscriber authorizes IdenTrust to verify Subscriber's identity and its ownership or lawful control of the domain name of Subscriber's server or other Internet device following the CAB Forum Baseline Requirements. IdenTrust may consult public or private databases or other sources for the purpose of verifying submitted information. In the event IdenTrust contacts Subscriber as part of such verification activities, Subscriber represents and warrants that any responses provided to IdenTrust by Subscriber as part of such contact shall be complete and accurate when given. IdenTrust will not request a credit report without Subscriber's express written prior consent, and this Agreement will not be construed as express written prior consent to obtain a credit report. Subscriber also authorizes IdenTrust to store and use in accordance with this Agreement any information generated during the application, identification, and certificate issuance processes.

3.4. Issuance. If IdenTrust accepts the application and confirms the information submitted, IdenTrust will create a TrustID Certificate in the name of Subscriber and the domain name(s) provided by Subscriber in the application, and will notify Subscriber how and where to retrieve such TrustID Certificate. When Subscriber retrieves such Server Certificate, Subscriber will be deemed to have been issued the Server Certificate by IdenTrust. If IdenTrust is unable to confirm Subscriber's identity and authorization, IdenTrust may refuse to approve Subscriber's application or refuse to issue a TrustID Certificate to Subscriber without any liability to any person or entity.

3.5. Acceptance. When Subscriber downloads the Server Certificate described in Section 3.4 above, the contents of such Server Certificate will be presented, and Subscriber agrees to (i) review again the information in the Server Certificate, and (ii) immediately notify IdenTrust of any inaccuracies, errors, defects or other problems with the Server Certificate. Subscriber agrees that it will have accepted the Server Certificate: (i) when it uses the Server Certificate or the corresponding Key Pair after downloading that Server Certificate, or (ii) if it fails to notify IdenTrust of any inaccuracies, errors, defects or other problems with the Server Certificate within a reasonable time after downloading it. Subscriber agrees to install the Server Certificate only on the server(s) accessible at the domain name listed on the Certificate and not to install or use such Server Certificate until it has reviewed and verified the accuracy of the data in such Certificate.

3.6. Term. The term of this Agreement commences upon Subscriber's Acceptance hereof. If the Application is not approved by IdenTrust, this Agreement will terminate upon such event. In the event a Server Certificate is issued by IdenTrust hereunder, then (a) the term of this Agreement shall terminate when the Server Certificate ceases to be valid, and (b) the Server Certificate will be valid for the Validity Period specified in the Server Certificate unless it ceases to be valid at an earlier time due to it being revoked as provided for herein. Subscriber hereby requests and authorizes IdenTrust to send

email messages to Subscriber relating to lifecycle events of Server Certificates (e.g., revocation events, reminding Subscriber of the renewal process).

4. Subscriber's Rights and Responsibilities.

4.1. Fee. Subscriber will be responsible for the applicable certificate issuance fee, and authorizes the billing as indicated during the application process. If the application is not approved by IdenTrust, payment of the fee will be refunded where payment has actually been received by IdenTrust or not collected where payment information was provided to IdenTrust but not yet fully processed by IdenTrust. If the certificate issuance fee is not paid, IdenTrust may revoke the Server Certificate without any liability to any person or entity. Once a Server Certificate is issued by IdenTrust, refunds are not provided.

4.2. Representations and Warranties. By accepting the Server Certificate, Subscriber: (i) Accepts its contents and the responsibilities identified in this Agreement; and (ii) represents and warrants to IdenTrust and to each Relying Party that, (a) Subscriber rightfully holds the Private Key corresponding to the Public Key listed in the Server Certificate, (b) all representations made and information submitted by Subscriber to IdenTrust in the application process were current, complete, true and not misleading, (c) Subscriber has provided all facts material to confirming your identity and to establishing the reliability of the Server Certificate, (d) all information in the Server Certificate that identifies Subscriber is current, complete, true and not misleading, (e) Subscriber is not aware of any fact material to the reliability of the information in the Server Certificate that has not been previously communicated to IdenTrust, and (f) Subscriber has kept its Private Key secret.

4.3. Use of the Server Certificate. The Server Certificate may be used by servers and other Internet devices to establish secure communications sessions with third parties. The Server Certificate may not be used: (i) for any application requiring fail-safe performance, such as the operation of nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems, or any other system whose failure could lead to injury, death or environmental damage; (ii) for transactions where applicable law prohibits its use or where otherwise prohibited by law; (iii) for fraud or any other illegal scheme or unauthorized purpose; (iv) to present, send or otherwise transfer hostile code, including spyware or other malicious software; (v) in any software or hardware architectures that provide facilities for interfering with encrypted communications; (vi) on any server or other Internet device that is not located on the Internet at a domain name owned or lawfully controlled by Subscriber and contained in the Server Certificate; or (vii) to issue any other Certificate.

4.4. Protect Private Key. Subscriber is responsible for protecting its Private Key. Subscriber represents, warrants and agrees that, in regard to the Server Certificate, Subscriber: (i) has kept and will keep its Private Key (and any Activation Data used to protect Subscriber's Private Key) private, and (ii) will take reasonable security measures to prevent unauthorized access to, or disclosure, loss, modification, compromise, or use of, its Private Key and the computer system or media on which its Private Key is stored.

Subscriber may change its employee(s) or agent(s) who are authorized to use and administer on behalf of Subscriber the Server Certificate, without requesting revocation of the current Server Certificate, but Subscriber shall bear the security and control risks associated with making such changes without revoking the Server Certificate. In the alternative, Subscriber may request revocation of the current Server Certificate and apply for a new TrustID Certificate, subject to the fees and other requirements associated with the issuance of a new TrustID Certificate. Subscriber agrees that the act or omission of any employee or agent of Subscriber who has access to use the Server Certificate or the corresponding Private Key, in using or administering the Server Certificate or such Private Key, will be deemed for all purposes to be the act or omission of Subscriber

Failure to protect the Private Key or to notify IdenTrust of the theft, compromise, or misuse of the Private Key may cause Subscriber serious adverse legal and financial consequences.

If Subscriber ever suspects or discovers that the security of its Private Key has been or is in danger of being compromised in any way, Subscriber must immediately notify IdenTrust, as provided in Section 4.7 below, and request that the Server Certificate be revoked.

4.5. Changes in Certificate Information. If any information in the Server Certificate changes, Subscriber must immediately notify IdenTrust as provided in Section 4.7 below.

4.6. Responsiveness to Instructions. Subscriber must respond to IdenTrust within 12 hours if IdenTrust sends instructions to Subscriber regarding any actual or possible compromise of Subscriber's Private Key or misuse of the Server Certificate.

4.7. Revoke the Server Certificate

When to Revoke the Server certificate

Subscriber must immediately request that a Server Certificate be revoked if: (i) the Subscriber's corresponding Private Key has actually been, or is suspected of being lost, disclosed, compromised or subjected to unauthorized use in any way; or (ii) any information in the Server Certificate is no longer accurate, current, or complete or becomes misleading. Subscriber may also revoke any Server Certificate at any time for any other reason by following the guidelines below.

How to Revoke the Server Certificate

When submitting a Server Certificate revocation request, Subscriber warrants that such request is handled following IdenTrust guidelines to report certificate security compromise issues published at: https://www.identrust.com/report-certificate-security-compromise-issues, as may be amended from time to time with or without notice. Subscriber warrants that Subscriber will provide one corresponding revocation reason code as documented in the guidelines of the aforementioned webpage.

Subscriber is hereby informed, and acknowledges understanding, of the reasons for revoking a Server Certificate, which are also further explained in Section 4.9.3 of the TrustID CPS or TLS CP-CPS, incorporated herein by reference and made a part of this Agreement.

Subscriber can initiate a revocation request for a given Server Certificate by using any of the below options:

1) sending an email to Support@identrust.com, which email contains the reason for revocation based on the description supplied at https://www.identrust.com/report-certificate-security-compromise-issues, as may be amended from time to time with or without notice, and is signed using the Private Key corresponding to such Server Certificate;
2) calling IdenTrust Support toll free within the U.S. at 1 (888) 339-8404 or from outside of the U.S. at 1 (801) 384-3481;
3) online-request via IdenTrust's online certificate management interface systems, if such systems are made available to Subscriber and Subscriber has signed up for access to such IdenTrust online systems, which such availability and access, if any, are outside the scope of this agreement; or
4) such other means as may be provided by IdenTrust

4.8. Cease Using the Server Certificate. Subscriber must immediately cease using the Server Certificate in the following circumstances: (i) the Subscriber's Private Key (corresponding to the Public Key listed in the Server Certificate) has actually or is suspected of being lost, disclosed, compromised or subjected to unauthorized use in any way; (ii) when any information in the Server Certificate is no longer accurate, current, or complete or becomes misleading; (iii) upon the revocation or expiration of the Server Certificate; or (iv) upon termination of this Agreement.

4.9. Indemnification. Subscriber agrees to indemnify and hold IdenTrust and its directors, officers, employees, agents and affiliates harmless from any and all liabilities, costs, and expenses, including reasonable attorneys' fees, related to: (i) any misrepresentation or omission of material fact by Subscriber or its employees or agents to IdenTrust, whether or not such misrepresentation or omission was intentional; (ii) Subscriber's violation of this Agreement; (iii) any compromise or unauthorized use of the Server Certificate (or the corresponding Private Key) caused by Subscriber's negligence, intentional misconduct or breach of this Agreement, unless prior to such unauthorized use Subscriber has appropriately requested revocation of the Server Certificate and proven its authority to request revocation; or (iv) Subscriber's misuse of the Server Certificate, including without limitation any use of the Server Certificate that is not permitted by this Agreement.

5. IdenTrust's Rights and Responsibilities.

5.1. Privacy. With respect to Private Information provided by Subscriber to IdenTrust in connection with this Agreement, IdenTrust will care for and process such information in accordance with the Privacy Policy.

Subscriber acknowledges that information contained in TrustID Certificates and related status information shall not be considered or deemed Private Information--that would defeat the purpose of the Server Certificate, which is to establish a trusted, secure communication link between Subscriber's server(s) located at the domain names of Subscriber included in the Server Certificate and third parties, and to confirm the identity of Subscriber and Subscriber's control of the domain names(s) of Subscriber identified in the Server Certificate. Subscriber authorizes the use of such information in furtherance of the purposes of this Agreement and in conformity with the requirements of the TrustID CP, CPS, or TLS CP-CPS.

5.2. Certificate Repository. During the term of this Agreement, IdenTrust will operate and maintain a secure online repository that contains (i) all current, valid TrustID Certificates (including, as applicable, the Server Certificate), and (ii) a CRL or online database indicating the status, whether valid, suspended or revoked, of TrustID Certificates. When Subscriber accepts the Server Certificate, IdenTrust will publish the Server Certificate in the repository and will indicate its valid status until it is suspended, revoked or expired.

5.3. Revocation. IdenTrust may revoke the Server Certificate when any party makes a claim against IdenTrust that the Server Certificate is invalid or has been compromised.

IdenTrust will revoke the Server Certificate upon request and update the Repository as soon as practical after IdenTrust has adequately confirmed that the person making the revocation request is authorized to do so. If the request is signed using the Private Key corresponding to the Server Certificate, IdenTrust will accept the request as valid.

IdenTrust may also revoke the Server Certificate without advance notice if it determines, in its sole discretion, that: (i) the Server Certificate was not properly issued or was obtained by fraud; (ii) the security of the Private Key corresponding to the Server Certificate has or may have been lost or otherwise compromised; (iii) the Server Certificate has become unreliable; (iv) material information in the application or the Server Certificate has changed or has become false or misleading; (v) Subscriber has violated any applicable agreement or obligation; (vi) Subscriber requests revocation; (vii) a governmental authority has lawfully ordered IdenTrust to revoke the Server Certificate; (viii) this Agreement terminates; (ix) the trust status of IdenTrust is compromised or at risk of compromise if the Server Certificate is not revoked; or (x) there are other reasonable grounds for revocation, including any violation of a provision of the TrustID CP, CPS, TLS CP-CPS or CAB Forum Baseline Requirements by the Subscriber or by IdenTrust. IdenTrust will notify Subscriber when the Server Certificate has been revoked.

5.4. Warranties. Subject to the provisions in the TrustID CP, CPS, or TLS CP-CPS and this Agreement, and Subscriber's fulfillment of its duties and obligations under the same, IdenTrust warrants: (i) that the Server Certificate shall be issued and managed in accordance with the applicable terms of the TrustID CP, CPS or TLS CP-CPS and this Agreement; and (ii) that the Server Certificate meets all requirements of the TrustID CP, CPS, or TLS CP-CPS and this Agreement.

5.5. Disclaimer of Warranties and Limitations of Liability. EXCEPT AS PROVIDED IN SECTION 5.4 ABOVE, THE SERVER CERTIFICATE IS PROVIDED BY IDENTRUST "AS-IS" AND IDENTRUST DISCLAIMS ANY AND ALL WARRANTIES OF ANY TYPE, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, CORRECTNESS OR ACCURACY OF INFORMATION PROVIDED, OR FITNESS FOR A PARTICULAR PURPOSE, WITH REGARD TO THE SERVER CERTIFICATE AND ANY IDENTRUST SERVICE. IDENTRUST MAKES NO WARRANTY THAT THE SERVER CERTIFICATE OR ANY IDENTRUST SERVICE WILL MEET ANY EXPECTATIONS, OR THAT ANY FUNCTION OR AVAILABILITY THEREOF WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR FREE, OR THAT DEFECTS WILL BE CORRECTED. IDENTRUST MAKES NO WARRANTY REGARDING THE CONTENT OF ANY WEBSITE OR SERVER USING AN IDENTRUST SECURED SSL/TLS CERTIFICATE.

IN NO EVENT SHALL IDENTRUST'S LIABILITY ARISING FROM OR RELATED TO THIS AGREEMENT EXCEED AN AMOUNT EQUAL TO THE AMOUNT SUBSCRIBER ACTUALLY PAID IDENTRUST FOR THE SERVER CERTIFICATE FOR WHICH SUBSCRIBER APPLIED FOR IN CONNECTION WITH THIS AGREEMENT.

IDENTRUST WILL NOT BE LIABLE TO SUBSCRIBER UNDER ANY CIRCUMSTANCES WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES OF ANY KIND (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUE OR GOODWILL OR ANTICIPATED PROFITS OR LOST BUSINESS), REGARDLESS OF WHETHER IDENTRUST KNEW OR HAD REASON TO KNOW OF THE POSSIBILITY THEREOF.

THE PARTIES AGREE THAT THE FOREGOING LIMITATION OF WARRANTIES AND LIABILITY ARE AN ESSENTIAL INDUCEMENT TO IDENTRUST TO ENTER INTO THIS AGREEMENT, AND THAT THE FOREGOING LIMITATIONS SHALL APPLY TO THE GREATEST EXTENT PERMITTED BY LAW.

6. Governing Law. The parties hereto agree that the United Nations Convention on Contracts for the International Sale of Goods will not apply to this Agreement. This Agreement shall be governed by and construed under the laws of the State of Utah, without regard to its conflicts of law principles.

7. Force Majeure. If IdenTrust's performance of any obligation under this Agreement is prevented or delayed by an event beyond such IdenTrust's reasonable control, including without limitation, crime, fire, flood, war, terrorism, riot, acts of civil or military authority (including governmental priorities), severe weather, strikes or labor disputes, or by disruption of telecommunications, power or Internet services not caused by such IdenTrust, then IdenTrust will be excused from such performance to the extent it is necessarily prevented or delayed thereby.

8. Assignment. Subscriber may not assign this Agreement or delegate any obligations hereunder. Any attempt by Subscriber to assign this Agreement or delegate any obligations hereunder shall render this Agreement voidable by IdenTrust, in its sole discretion. IdenTrust may assign this Agreement or delegate all or part of its obligations hereunder upon: (i) notice to Subscriber; or (ii) assignment of all rights and obligations hereunder to a successor in interest, whether by merger, sale of assets or otherwise.

9. Notice. Notice from Subscriber to IdenTrust shall be effective upon actual receipt by IdenTrust and shall be made by either internationally recognized overnight courier service or by certified mail addressed to:

IdenTrust Services, LLC
Attn: Legal Department
5225 W Wiley Post Way, Ste 450
Salt Lake City, UT 84116-2898

Notices from IdenTrust to Subscriber shall be made by posting on the Repository, or by mail or email in the event IdenTrust receives an email or mailing address for Subscriber in the course of communications made in connection with this Agreement. Except as otherwise provided herein, notices to Subscriber posted on the Repository shall be deemed effective three (3) days after being so posted, notices to Subscriber sent by mail shall be deemed effective seven (7) days after being sent, and notices to Subscriber sent by email shall be deemed effective when sent.

10. Dispute Resolution. In the event of any dispute or disagreement between the parties hereto ("Disputing Parties") arising out of or related to this Agreement or any Server Certificate, the Disputing Parties will use their best efforts to settle the dispute or disagreement through mediation or good faith negotiations following notice from one Disputing Party to the other. If the Disputing Parties cannot reach a mutually agreeable resolution of the dispute or disagreement within sixty (60) days following the date of such notice, then the Disputing Parties will submit the dispute to binding arbitration, as provided below.

Except for a controversy, claim, or dispute involving the federal government of the United States or a "Core Proceeding" under the United States Bankruptcy Code, the parties agree to submit any controversy, claim, or dispute, whether in tort, contract, or otherwise arising out of or related in any way to this Agreement, that cannot be resolved by mediation or negotiations between the parties, for resolution by binding arbitration by a single arbitrator, and judgment upon the award rendered by the arbitrator may be entered in any court having jurisdiction over the parties. The arbitrator will have no authority to impose penalties or award punitive damages. Binding arbitration will: (i) proceed in Salt Lake County, Utah; (ii) be governed by the Federal Arbitration Act (Title 9 of the United States Code); and (iii) be conducted in accordance with the Commercial Arbitration rules of the American Arbitration Association ("AAA"). Each party will bear its costs for the arbitration; however, upon award of any judgment or conclusion of arbitration, the arbitrator will award the prevailing party the costs it expended in such arbitration. Unless the arbitrator otherwise directs, the parties, their representatives, other participants, and the arbitrator will hold the existence, content, and result of the arbitration in confidence. This arbitration requirement does not limit the right of any party to obtain provisional ancillary remedies such as injunctive relief or the appointment of a receiver, before, during, or after the pendency of any arbitration proceeding. This exclusion does not constitute a waiver of the right or obligation of any party to submit any dispute to arbitration.

11. Relationship Of The Parties. Nothing in this Agreement shall be deemed to create a partnership or joint venture or fiduciary relationship, and neither party is the other's agent, partner, employee or representative.

12. Headings And Titles. The headings and titles contained in this Agreement are included for convenience only, and will not limit or otherwise affect the terms of this Agreement.

13. Waiver. No waiver by either party of any default will operate as a waiver of any other default, or of a similar default on a future occasion. No waiver of any term or condition by either party will be effective unless in writing and signed by the party against whom enforcement of such waiver is sought.

14. Severability. In case one or more of the provisions of this Agreement should be held invalid, illegal or unenforceable in any respect for any reason, the same will not affect any other provision in this Agreement, which will be construed to give maximum effect to the extent of the parties as evidenced by this original Agreement as originally drafted save to the extent of such invalid, illegal or unenforceable provision.

15. Entire Agreement. This Agreement, including the TrustID CP, CPS, or TLS CP-CPS as referenced herein, represents the entire agreement of the parties, and supersedes all other agreements and discussions relating to the subject matter hereof. Except as expressly provided otherwise in this Agreement, this Agreement may not be amended except in writing signed by both parties.

16. Third Party Beneficiaries. Each Application Software Supplier and each Relying Party is an intended third party beneficiary of Subscriber's representations, warranties and obligations made herein.

17. Amendment. You agree that this Agreement, the TrustID CP, CPS, or TLS CP-CPS can be amended from time to time by IdenTrust, in its sole discretion. Any such modifications shall be effective immediately upon a revised version of the applicable document being posted by IdenTrust to the Repository. If Subscriber uses the Server Certificate hereunder after such a posting, Subscriber shall be deemed to have accepted the most recent versions of the Agreement, the TrustID CP,

CPS or TLS CP-CPS posted on the Repository and be bound thereunder. You are responsible for periodically checking the Repository for the latest version of the Agreement, the TrustID CP, CPS or TLS CP-CPS posted on the Repository.

18. Survival. Sections governing confidentiality of information, indemnification, disclaimer of warranties, limitations of liability, governing law and dispute resolution will survive any termination or expiration of this Agreement.

19. Definitions and Terms.

Accept or Acceptance: An End Entity's act that triggers the End Entity's rights and obligations with respect to its TrustID Certificate under the applicable Certificate Agreement or Authorized Relying Party Agreement. Indications of Acceptance may include without limitation: (i) using the TrustID Certificate (after Issuance); failing to notify IdenTrust of any problems with the TrustID Certificate within a reasonable time after receiving it; or other manifestations of assent.

Activation Data: Private data used to access or activate Cryptographic Modules (e.g., a personal identification number (PIN), pass phrase, or a manually-held Key share used to unlock a Private Key prior to creating a Digital Signature).

Agreement: Refers to these Terms and Conditions as incorporated into the TRUSTID IDENTRUST | TLS/SSL | ORGANIZATION IDENTITY | ORGANIZATION VALIDATED (OV) CERTIFICATE SUBSCRIBER AGREEMENT signed by Subscriber.

Applicant: An Individual or Organization that submits application information to an RA or an Issuing CA for the purpose of obtaining, renewing or a request to revoke a TrustID Certificate.

Application Software Supplier: A supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates Root Certificates.

Application: Means the online application for a TrustID Certificate made in connection with this Agreement, and, if any, each request for a TrustID Certificate made by an Applicant.

Authorized Relying Party Agreement: A contract between an Individual or an Organization and IdenTrust allowing the party to rely on TrustID Certificates in accordance with the TrustID CP, CPS or TLS CP-CPS.

CAB Forum Baseline Requirements: The current version of the "Baseline Requirements for the Issuance and Management of Publicly- Trusted-Certificates" published at: https://cabforum.org/working-groups/server/baseline-requirements/requirements

Certificate: A computer-based record or electronic message that: (i) identifies the Certification Authority issuing it; (ii) names or identifies a Subscriber, Authorized Relying Party or Electronic Device; (iii) contains the Public Key of the Subscriber, Authorized Relying Party or Electronic Device; (iv) identifies the Certificate's Validity Period; (v) is Digitally Signed by a Certification Authority and (vi) has the meaning ascribed to in accordance with applicable standards. A Certificate includes not only its actual content but also all documents expressly referenced or incorporated in it.

Certificate Policy (CP): A named set of rules that indicates the applicability of Certificates to particular communities and classes of applications and specifies the Identification and Authentication processes performed prior to Certificate Issuance, the Certificate Profile and other allowed uses of Certificates.

Certificate Profile: The protocol used in Section 7 of the TrustID CPS or TLS CP-CPS, and the TrustID Certificate Profile document to establish the allowed format and contents of data fields within TrustID Certificates, which identify IdenTrust as the Issuing CA, the End Entity, the Certificate's Validity Period, and other information that identifies the End Entity.

Certification Authority (CA): An entity that creates, issues, manages and revokes Certificates.

Certification Practice Statement (CPS): A statement of the practices that a CA employs in creating, issuing, managing and revoking Certificates.

CRL: A database or other list of Certificates that have been revoked prior to the expiration of their Validity Period.

Cryptographic Module: The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [NIST FIPS 140-3].

Digital Signature/Digitally Sign: The transformation of an electronic record by one person, using a Private Key and Public Key Cryptography, so that another person having the transformed record and the corresponding Public Key can accurately determine (i) whether the transformation was created using the Private Key that corresponds to the Public Key, and (ii) whether the record has been altered since the transformation was made.

Electronic Device: Computer software, hardware or other electronic or automated means (including email) configured and

enabled by a person to act as its agent and to initiate or respond to electronic records or performances, in whole or in part, without review or intervention by such person.

End Entity: Subscribers and Authorized Relying Parties.

Government Entity: A Legal A Legal Entity, the existence of which was established by the government of a nation or a political subdivision thereof and is owned or controlled by such government or political subdivision.

Identification and Authentication: The process by which IdenTrust ascertains and confirms through appropriate inquiry and investigation the identity of the Subscriber and, if applicable, representatives of Subscriber. Certain aspects and activities within this process are prescribed by the TrustID CP and CPS. or TLS CP-CPS.

Individual: A natural person and not a juridical person or Legal Entity.

Internet: A global system of interconnected computer networks that uses multiple protocols to communicate data.

Key Pair: Two mathematically related keys (a Private Key and its corresponding Public Key), having the properties that (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, Government Entity or other entity with legal standing in a country's legal system.

Organization: An entity that is legally recognized in its jurisdiction of origin (e.g., a corporation, partnership, sole proprietorship, government department, non-government Organization, university, trust, special interest group or non-profit corporation).

Privacy Policy: The policy posted at www.identrust.com/privacy.html, which may be amended from time to time by IdenTrust in its sole discretion.

Private Information: Non-public information that Subscriber provides or that IdenTrust obtains, during the application and Identification and Authentication processes, that is not included in the Server Certificate and that identifies Subscriber.

Private Key: The key of a Key Pair kept secret by its holder and used to create Digital Signatures and to decrypt messages or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair publicly disclosed by the holder of the corresponding Private Key and used by the recipient to validate Digital Signatures created with the corresponding Private Key and to encrypt messages or files to be decrypted with the corresponding Private Key.

Public Key Cryptography: A type of cryptography (a process of creating and deciphering communications to keep them secure) that uses a Key Pair to securely encrypt and decrypt messages. One key encrypts a message, and the other key decrypts the message. One key is kept secret (Private Key), and one is made available to others (Public Key). These keys are, in essence, large mathematically-related numbers that form a unique pair. Either key may be used to encrypt a message, but only the other corresponding key may be used to decrypt the message.

Public Key Infrastructure (PKI): The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based Public Key Cryptography system.

Relying Party: A person or Legal Entity who has received information that includes a Certificate and a Digital Signature verifiable with reference to a Public Key listed in the Certificate, and is in a position to rely on them.

Repository: The information and data repository of IdenTrust located at:

https://www.identrust.com/support/documents/trustid

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Server Certificate: The TrustID | Organization Identity | Organization Validated (OV) Certificate issued to Subscriber pursuant to this Agreement.

Subscriber: The entity for which the Application is made, and which is identified to IdenTrust in such Application, and which is identified within the "subject:organizationName" (as defined in the CAB Forum Baseline Requirements) field of the Server Certificate that is the subject of this Agreement.

Subscriber Agreement: See Agreement.

TLS CP-CPS: A consolidated CP and CPS document in which the CA's certificate applicability rules and its operational practices are defined together under one overarching framework.

TrustID Certificate: A Certificate issued by IdenTrust under the TrustID brand.

Validity Period: The intended term of validity of a Server Certificate, beginning with the date of issuance ("Valid From" or "Activation" date), and ending on the expiration date indicated in the Server Certificate ("Valid To" or "Expiry" date).

Close window