COMMSCOPE®

CommScope Digital Certificate Subscriber Agreement for Publicly Trusted Certificates

Document Number: PR5120
Revision: v1.1
Revision Date: 7-18-2022

Table of Contents

Contents

1 Contact Information and Signatures

This Digital Certificate SubscriberAgreement ("Agreement"), is made effective as of _____ (the "Effective Date") by and between CommScope, Inc. of North Carolina (referred to from here on as CommScope) with offices at 6450 Sequence Drive, San Diego, CA 92121 and the party identified below ("Subscriber").

Subscriber: (Legal Entity executing this Agreement)	Billing Contact:	
Address:	Title:
	Phone:
	Fax:
	E-mail:
Technical Contact:	Legal Contact:
Title:	Title:
Phone:	Phone:
Fax:	Fax:
E-mail:	E-mail:

CommScope grants the Subscriber the authorization to obtain and utilize the Digital Certificates and corresponding private keys in accordance with the terms and conditions of this Agreement as well as in accordance with the following specifications:

[1] CommScope Certificate Policy and Certification Practice Statement ("CP/CPS"), PR5031, published at: http://certificates.pkiworks.com/Public/Documents/.

[2] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, https://cabforum.org/baseline-requirements-documents/, Browser Forum.

[3] Network and Certificate System Security Requirements, https://cabforum.org/network-security/, Browser Forum.

SUBSCRIBER HAS READ AND AGREES TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT, <u>INCLUDING THOSE TERMS CONTAINED ON THE FOLLOWING PAGES HEREOF</u>.

In consideration of the mutual promises and covenants contained herein, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties have entered into this Agreement as of the Effective Date.

COMMSCOPE, INC. OF NORTH CAROLINA	SUBSCRIBER NAME:
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:

2   Definitions, Abbreviations and Acronyms

All capitalized terms used herein but not defined below shall have the meanings assigned to them in section 1.6 of the CommScope CP/CPS [1].

Application Software Supplier	A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.
Certificate Manager	A service manager identified by CommScope that manages certain aspects of the Publicly-Trusted Certificate Authorities.
Compliant	In full accordance with all of the applicable requirements that are stated in [1].
Digital Certificate	Digital Certificates covered by this agreement are specified in Exhibit A.
Digital Certificate Private Key	A private key that cryptographically corresponds to the Digital Certificate issued to the Subscriber. A digital signature generated with this private key can be validated with the public key inside the Digital Certificate.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
Subject	The user of the end-entity Digital Certificate issued under this agreement with direct or indirect access to the corresponding Digital Certificate Private Key.
Wrongful Use	Subscriber has knowingly or with gross negligence embedded a Digital Certificate or a corresponding Digital Certificate Private Key in a device, computer system or any other product or application that is not Compliant.

3   Digital Certificate Authorization

Upon receipt of a complete and executed Agreement, payment of appropriate fees (contact PKI.Center@commscope.com for current pricing information), the Subscriber's information and Naming Documents (see **Exhibit A**), and verification of Subscriber's identity for security purposes, CommScope hereby authorizes Subscriber to receive Digital Certificates issued from a CommScope Publicly-Trusted CA while the Agreement is in effect.

4   Subscriber Representations and Warranties

In the event that Subscriber is in breach of any of its representations and warranties, as set forth below in this Section 4 , CommScope may, at CommScope's sole discretion revoke Subscriber's Digital Certificates and/or terminate this Agreement.

Subscriber hereby represent and warrants the following:

4.1 Embedding of Digital Certificates. Subscriber shall not embed or otherwise use the Digital Certificates in any manner that is illegal or not Compliant. Subscriber shall not embed or otherwise use any Digital Certificate associated with a private key that Subscriber knows or should have known was stolen, intercepted or otherwise compromised in any way.

4.2 Security of Digital Certificate Private Keys. Subscriber shall safeguard the Digital Certificate Private Keys to ensure that the private keys are not lost, stolen, embedded or otherwise used in a product which is not Compliant or otherwise used in a manner that may compromise or actually does compromise the Private Key and corresponding Subscriber Certificate, as determined by CommScope in accordance with [1] .

4.3 Request/Receipt of Digital Certificates. Within thirty (30) days after receipt of the annual maintenance fee (contact PKI.Center@commscope.com for current pricing information), for end entity certificate services, CommScope shall cause the Certificate Manager to send to Subscriber certain secure software and an administrator token for securely obtaining Digital Certificates in an automated fashion. Subscriber shall install and use the software and administrator token to submit requests for, and receive, Digital Certificates in accordance with CommScope applicable process and procedures.

4.4 Non-repudiation. Each digital signature created using the Digital Certificate Private Key is the digital signature of the Subscriber whenever the Digital Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created.

4.5 Accurate Subscriber Information. All representations made by the Subscriber in the Certificate Application and within each individual Digital Certificate request the Subscriber submitted are true. Subscriber shall review and verify the Certificate contents for accuracy.

4.6 Restriction on End Entity Certificates. When Subscriber is issued an end entity Digital Certificate, the corresponding private key shall not be used under any circumstances to digitally sign any kind of digital certificate or any kind of a message or data structure containing a public key. Furthermore, the end entity's private key shall never be used to sign CRLs and shall not be utilized in any manner representing a Certificate Authority. Certificate shall be installed only on servers that are accessible at the subjectAltName(s) listed in the Certificate.

4.9 Subject Training. Before requesting the issuance of a certificate for a Subject, Subscriber shall train the Subject according to the Baseline Requirements [2] on the importance of Private Key security so that the Subject has the know-how to protect their Private Key to prevent its compromise, loss, or unauthorized use. Subscriber shall also make Subject aware that Subject is to notify Subscriber in the event of Subject's loss of their Private Key or suspicion of compromise or unauthorized use of their Private Key.

4.10 Prompt notification. The Subscriber shall promptly notify CommScope upon any of the following events occurring:

- Suspicion of loss or compromise of their private key(s)
- Any other known violations of any of the Subscriber representations and warranties listed in this section
- Any information in the Certificate is or becomes incorrect or inaccurate.

4.11 Material Changes. The Subscriber shall notify the CA of any material changes to their organization name, company's legal status, address or contact information within 3 business days of any such occurrence.

4.12 Key Compromise. Subscriber shall respond to the CA's instructions concerning Key Compromise or Certificate misuse within 24 hours.

4.12 Certificate Revocation. Subscriber acknowledges and accepts that the CA is entitled to revoke the certificate immediately if the Subscriber were to violate the terms of the Subscriber Agreement, due to a Key Compromise, if the information in the Certificate is or becomes invalid, or if revocation is required by the CommScope CP/CPS [1] for any other reason. Subscriber shall immediately cease using a Certificate, after either the Subscriber or CommScope CA determine that revocation is required.

5. No Other Rights

CommScope retains all right, title, and interest in and to the CommScope-operated Publicly-Trusted root certificates and any associated trade secrets or other proprietary information associated therewith that is provided by CommScope to Subscriber hereunder. CommScope grants no rights in any trademark, trade name, service mark, business name or goodwill of CommScope. Subscriber shall not modify, create derivative works, reverse engineer, decompile, disassemble or in any manner attempt to derive the source code from any software or tools provided by CommScope in whole or in part

6 Idemnity, Warranty and Limitation of Liability

6.1 Indemnification. Subscriber shall indemnify and hold harmless CommScope and its employees that operate the Publicly-Trusted Root CAs and Sub-CAs that issued Subscriber Certificates, for any claim or damage arising from or related to:

- Falsehood or misrepresentation of fact by the Subscriber on its Certificate Application or within individual certificate requests.
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party.
- The Subscriber's failure to take the precautions necessary to prevent the compromise, loss, disclosure, modification, or Wrongful Use of the Subscriber's private key(s).
- The Subscriber's use of a name (including such a name that infringes upon the Intellectual Property Rights of a third party)

CommScope shall notify Subscriber, in writing of any such claim and (ii) Subscriber shall have the sole control of the defense and all negotiations for any settlement or compromise of such claim, provided, however, that CommScope may participate in such defense using counsel of its own choice and at its sole expense.

6.2 Disclaimer of Warranties. THE DIGITAL CERTIFICATES, USE OF WHICH IS AUTHORIZED HEREUNDER, ARE PROVIDED "AS IS" AND COMMSCOPE DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUIET ENJOYMENT, ACCURACY, SECURITY, OR NON-INFRINGEMENT.

6.3 Limitation of Liability. WITH THE EXCEPTION OF SUBSCRIBER's INDEMNIFICATION OBLIGATIONS, SUBSCRIBER's GROSS NEGLIGENCE, WILLFUL ACTS OR WRONGFUL USE, IN NO EVENT (i) WILL EITHER PARTY BE LIABLE UNDER THIS AGREEMENT FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR PUNITIVE DAMAGES INCLUDING, WITHOUT LIMITATION, DAMAGES WHICH REFLECT LOST BUSINESS, PROFITS OR REVENUE OBTAINED OR LOST, OR THE COSTS OF RECONSTRUCTING DATA OR REBUILDING DEVICES, WHETHER DAMAGES OF THIS NATURE WERE FORESEEABLE OR NOT, AND EVEN IF THAT PARTY HAD BEEN ADVISED THAT DAMAGES OF THIS NATURE WERE POSSIBLE; OR (ii) SHALL EITHER PARTY BE LIABLE UNDER THIS AGREEMENT TO THE OTHER PARTY FOR ANY AMOUNT EXCEEDING THE FEES ACTUALLY RECEIVED BY COMMSCOPE FROM SUBSCRIBER. COMMSCOPE DISCLAIMS LIABILITY TO THE SUBSCRIBER FOR ANY LOSSES OR DAMAGES OF ANY KIND SUFFERED AS A RESULT OF USE OR RELIANCE ON A CERTIFICATE BEYOND THOSE SPECIFIED IN THE COMMSCOPE CP/CPS.

6.4 Subscriber Liability for Subscriber Supplied Information. Subscriber is solely responsible for the resulting Digital Certificates created from the information Subscriber provides in the exhibits attached hereto and incorporated by this reference. Failure to completely and correctly complete the exhibits will result in incorrect Digital Certificates.

7   Term and Termination

7.1   Term. The term of this Agreement shall begin on the Effective Date and shall continue until terminated earlier under the provisions of this Section.

7.1 Termination by Subscriber. Subscriber may terminate this Agreement, with or without cause, by giving CommScope 180 day notice written notice of such termination.

7.2 Termination by CommScope. CommScope may terminate this Agreement, with or without cause, by giving Subscriber 180 day written notice of such termination. CommScope may also terminate this Agreement for material breach of this Agreement by Subscriber, where such breach is not cured within thirty (30) days of written notice to Subscriber; or, where such breach in incapable of cure at the time of the material breach. Examples of material breach include, but are not limited to: breach of Subscriber's Representations and Warranties in Section 4. or a series of non-material breaches of this Agreement by Subscriber. In addition,

CommScope may terminate this Agreement immediately upon receipt of a court or governmental agency order to revoke Subscriber's authorization,..

7.3 Effect of Termination or Certificate Revocation. If this Agreement is terminated, or a Digital Certificate is revoked, Subscriber shall discontinue using such Digital Certificate(s) and cease embedding or otherwise using such Digital Certificate(s) in any or all affected device(s), computer system(s) or any other product(s) or application(s). Subscriber shall keep secret or destroy any unused or revoked Digital Certificates and any associated private keys, and take such other action as is reasonably directed by CommScope. Notwithstanding any termination of this Agreement, any un-revoked Digital Certificate(s) used in device(s), computer system(s) or any other product(s) or application(s) that are no longer under the control of Subscriber shall be valid until the expiration of their validity period.

8   Fees

8.1 Fees. To be specified (annual and/or per certificate fee depending on the type and number of certificates required). For pricing updates, please contact PKI.Center@commscope.com. Subscriber shall pay all Fees to CommScope, in advance. CommScope may, upon thirty (30) days prior written notice, modify the Fees. CommScope shall not charge a fee as a condition of making a Digital Certificate available in a repository or otherwise making Digital Certificates available to Relying Parties

8.2 Refunds. Notwithstanding a termination of this Agreement, CommScope will not provide a refund of either annual fees or fees for already issued or ordered Certificates, except where errors were committed by CommScope and such errors were not the result of incorrect information provided by Subscriber.

8.3 Applicable Taxes. The Fees paid by Subscriber hereunder are exclusive of, and Subscriber shall pay, all sales, use, value added, excise, income tax, withholding tax, and other taxes or charges (other than income taxes) that may be levied upon either party by taxing authorities in connection with this Agreement (except for taxes based on Subscriber's employees) and shall pay all income taxes that may be levied upon Subscriber.

9   General

9.1 Force Majeure. No party (a **"Frustrated Party")** shall be liable to any other party (a **"Non-Frustrated Party")** for any failure to perform or delay in performance of its obligations under this Agreement caused by (a) act of God; (b) outbreak of hostilities, riot, civil disobedience, act of terrorism or disease; (c) the act of any governmental authority including revocation of any license or consent; (d) fire, explosion, lightning strike, storm (including but not limited to hurricanes and tornadoes) or flood; (e) theft, malicious damage, strike, lockout or industrial action of any kind (provided that the strike, lockout or industrial action was outside the reasonable control of the Frustrated Party); or (f) any causes or circumstances beyond the Frustrated Party's reasonable control (collectively, a **"Force Majeure Event").** The Frustrated Party shall promptly notify the Non-Frustrated Party of the nature and extent of the circumstances of the Force Majeure Event once known. In the event of a Force Majeure Event, the Frustrated Party shall forthwith establish and implement a plan that minimizes the disruption to the Non-Frustrated Party and shall use its commercially reasonable efforts to remedy the situation and remove the cause of its inability to perform as soon as possible. The Frustrated Party shall give the Non-Frustrated Party prompt notice of the cessation of the Force Majeure Event. The Frustrated Party and the Non-Frustrated Party shall negotiate in good faith adjustments to the terms and conditions of this Agreement that are equitable taking into account the nature and extent of the circumstances of the Force Majeure Event as they develop and become known

9.2   Notices. All notices, requests and other communications to any party hereunder shall be in writing and shall be given as follows:

If to Subscriber:

with a copy to:

If to CommScope:

pki.center@commscope.com

with a copy to:

> CommScope
> 101 Tournament Drive
> Horsham, PA 19044
> Attention: Vice President and Lead Counsel, Commercial Law Department

or to such other address, email address or facsimile number as such party may hereafter specify for the purpose by notice to the other parties hereto; provided that the parties acknowledge and agree that (a) notices may be sent by email to the most recent email address that the sender has on file for the applicable notice party specified above (b) notices sent by email shall be deemed delivered when sent and confirmed as received with no bounce-back and a follow-up telephone call, and (c) the parties shall use commercially reasonable efforts to update each other from time to time with the most current email addresses of their respective notice parties. All such notices, requests and other communications shall

be deemed received on the date of receipt by the recipient thereof if received prior to 5:00 p.m. in the place of receipt and such day is a business day in the place of receipt. Otherwise, any such notice, request or communication shall be deemed not to have been received until the next succeeding business day in the place of receipt.

9.3 Export. Subscriber shall not export or re-export (directly or, knowingly indirectly) any Digital Certificates, documentation, or other technical data without complying with the U.S. Export Administration Act and the associated regulations.

9.4 Waiver. Any waiver by either party hereto of any breach of this Agreement shall not constitute a waiver of any subsequent or other breach.

9.5 Survival. Subject to the terms and conditions of this Agreement, the obligations under this Agreement that by their nature or as specified under this Agreement are intended to continue beyond the termination, cancellation or expiration of this Agreement, including, without limitation and for the avoidance of doubt, the Subscriber's obligations under Sections 4 and 7 shall survive the termination, cancellation or expiration of this Agreement.

9.6 Assignment. Subscriber may not assign this Agreement without the express, prior written approval of CommScope.

9.7 Entire Agreement/Severability/Amendments. This Agreement embodies the entire understanding of the parties with respect to the subject matter hereof and merges all prior discussions between them, and neither of the parties shall be bound by any conditions, definitions, warranties, understandings or representations with respect to the subject matter hereof other than as expressly provided herein. If any provision or provisions of this Agreement shall be held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not be in any way affected or impaired thereby. No amendment or modification hereof shall be valid or binding upon the parties unless made in writing and signed by both parties hereto.

9.8 Governing Law; Forum. This Agreement shall be construed in accordance with the law of the state of New York, without regard to its conflict of laws rules. The Parties here by agree to exclusive jurisdiction and venue in the federal/state courts located in New York.

10   EXHIBIT A - Subscriber Information

SUBSCRIBER'S INFORMATION

CORPORATE INFORMATION:

Official Company Name:
Corporate Headquarters Address:
Headquarters Main Phone:
D-U-N-S Number:
Providing your DUNS number in advance can assist in the Authentication process. If you do not know your company's D-U-N-S number, you can look it up at http://www.dnb.com. Note: The Legal Company Name and Corporate Address listed above must match the information that is listed in the D-U-N-S Database.

SUBSCRIBER'S CORPORATE CONTACT:

This is the person responsible for the device manufacturing system, who is authorized to assign the other account contacts including administrators that will request Certificates from CommScope. Any authentications needed to approve or make changes to the account will all be authenticated through this Corporate Contact.

First Name:	Last Name:
Title:	E-mail:
Telephone:	Fax:

PRIMARY ADMINISTRATOR CONTACT:

This is the person who is authorized to request and receive certificates.

First Name:	Last Name:
Title:	E-mail:
Telephone:	Fax:
Address:	City and State:
Zip/Postal Code:	Country:

SECOND ADMINISTRATOR CONTACT:

This is the person who is authorized to backup the primary administrator contact. This person is also authorized to request and receive certificates.

First Name:	Last Name:
Title:	E-mail:
Telephone:	Fax:
Address:	City and State:
Zip/Postal Code:	Country:

SUBSCRIBER'S TECHNICAL CONTACT:

This is a technical contact, typically in development engineering, authorized to discuss technical issues related to Subscriber Certificates with CommScope.

First Name:	Last Name:
Title:	E-mail:
Telephone:	Fax:

SUBSCRIBER'S LEGAL CONTACT:

This person will receive a copy of any contractual related notices.

First Name:	Last Name:
Title:	E-mail:
Telephone:	Fax:
Address:	City and State:
Zip/Postal Code:	Country:

SUBSCRIBER'S BILLING CONTACT:

This is the person responsible for payment and notifying CommScope of any billing changes, for example an accounts payable representative.

First Name:	Last Name:
Title:	E-mail:
Telephone:	Fax:
Address:	City and State:
Zip/Postal Code:	Country:

Subscriber Publicly-Trusted Certificate Naming Application

CERTIFICATE FORMAT:

The Subscriber shall supply information required to generate Certificates by providing the information below:

Publicly-Trusted Certificate Profile Form	
Certificate type (select all that apply): ☐ Domain-Validated (DV) ☐ Organization-Validated (OV)	
Certificate usage (select one) ☐ SSL/TLS/HTTPS Server ☐ SSL/TLS/HTTPS Server and Client	
Organization Name Type (select one): ☐ Full legal name ☐ Abbreviation ☐ DBA/Trademark	
Provide documentation or a URL documenting that provided abbreviation is locally accepted:	
Subject DN[1]	c=<2-character country code>[2] o=<organization name (not to exceed 64 characters)>[3] ST=<state or province>[4] L=<locality name>[5]
Public Key Algorithm	<public key algorithm>[6]
Domain Names which may appear in Subscriber Certificates:	

---

[1] Only applicable to OV certificates. This section (Subject DN attributes) may be left blank for DV certificates.

[2] A 2-character (Alpha-2) ASCII country code compliant with ISO 3166, see https://www.iso.org/obp/ui/#search.

[3] Subscriber Organization Name, DBA or a common variations or abbreviations, provided that the Subscriber documents the difference. Any abbreviations used shall be locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", the Subscriber may specify "Company Name Inc." or "Company Name".

[4] The full state or province name (without any abbreviation) within which Subscriber's organization is authorized to conduct business.

[5] The full name of a city or a town within which Subscriber's organization is authorized to conduct business.

[6] Algorithms include 2048-bit RSA and seccp256r1 ECDSA