



DIGITAL CERTIFICATE SUBSCRIBER AGREEMENT
WBA WRIX Certificate Authority

This Digital Certificate Subscriber Agreement (“Agreement”), is made effective as of _____ (the “Effective Date”) by and between Kyrio, Inc., a trade name of NetworkFX, Inc., a Delaware corporation with offices at 858 Coal Creek Circle, Louisville, Colorado 80027-9750, PHONE: 303-661-3438; FAX: 303-664-8156 and the party identified below (“Subscriber”).

Subscriber: (Legal name of the company)	Billing Contact:
Address:	Title:
	Phone:
	E-mail:
Technical Contact:	Legal Contact:
Title:	Title:
Phone:	Phone:
Email:	Email:

Kyrio is under contract with the Wireless Broadband Alliance (“WBA”) to act as a Certificate Authority to validate Subscriber and provide Certificates, through a third party, including Certificate Authorities, that Subscriber may be installed into systems in conformance to the WBA Certificate Policy.

Subscriber desires to obtain one or more of the Certificates or Certificate Authorities described hereunder. Subscriber is also knowledgeable of the WBA Certificate Policy which governs the use of the aforementioned Certificates and Certificate Authorities.

Kyrio, on behalf of WBA, hereby grants to Subscriber authorization to obtain and embed Certificates into compliant systems in accordance with the terms and conditions of this Agreement.

Please provide a check mark for the type of certificates you wish to obtain.
Only checked Exhibits need to be digitally signed.

WBA WRIX Certificates Types	Trial (120 day) WBA WRIX Certificates Types
<input type="checkbox"/> WRIX Server-Client End-Entity (Exhibit B)	<input type="checkbox"/> Trial WRIX Server-Client End-Entity (Exhibit F)
<input type="checkbox"/> WRIX Server Only End-Entity (Exhibit C)	<input type="checkbox"/> Trial WRIX Server Only End-Entity (Exhibit G)
<input type="checkbox"/> WRIX Client Only End-Entity (Exhibit D)	<input type="checkbox"/> Trial WRIX Client Only End-Entity (Exhibit H)
<input type="checkbox"/> WRIX Agent (RA Agent) (Exhibit E)	

If Subscriber makes use of the Certificate, as defined hereunder, either as an Access Network Provider (ANP), or Identity Provider (IDP) or both, described in the agreements referenced below, in connection with its participation in the OpenRoaming Federation, in signing this Agreement Subscriber agrees to the terms of the following agreements:

OpenRoaming ANP Program Agreement:
<https://wballiance.com/wp-content/uploads/2021/03/OR-ANP-Agreement-Baseline-Kyrio-20210317-v1.pdf>

OpenRoaming IDP Program Agreement:
<https://wballiance.com/wp-content/uploads/2021/03/OR-IDP-Agreement-Baseline-Kyrio-20210317-v1.pdf>

In the event either of the OpenRoaming ANP Program Agreement or OpenRoaming IDP Program Agreement are amended and Kyrio receives notice of such amendment from the OpenRoaming Federation then Kyrio will send Subscriber notice of the changed agreement and access to the terms of such new agreement. If Subscriber does not approve the new terms, Subscriber may terminate this Agreement, which will then include termination of the OpenRoaming ANP Program Agreement and/or OpenRoaming IDP Program Agreement.

BY SIGNING THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU ARE AN AUTHORIZED REPRESENTATIVE OF SUCH ENTITY AND HAVE THE AUTHORITY TO ACCEPT THIS AGREEMENT ON SUCH ENTITY’S BEHALF. TYPICALLY, THIS IS AN EMPLOYEE WITH A VICE PRESIDENT (VP) OR HIGHER TITLE, AS AN OFFICER OF THE ENTITY. IF YOU DO NOT HAVE SUCH AUTHORITY OR IF YOU DO NOT ACCEPT THIS AGREEMENT, YOU SHOULD NOT SIGN BELOW.

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

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.

KYRIO, INC.	SUBSCRIBER:
Signature:	Signature:
Name:	Name:
Title:	Title:

Agreement

1.0 Definitions

- 1.1. Any definitions not provided in this agreement are defined in the WBA Certificate Policy. Some definitions are copied over to this agreement from the current WBA Certificate Policy as a convenience.
- 1.2. “Certificate” means, as defined in the current WBA Certificate Policy, a digital representation of information which at least:
 - 1.2.1. Identifies its issuing Certificate Authority (CA)
 - 1.2.2. Names or identifies the Subscriber of the Certificate
 - 1.2.3. Contains the Subscriber’s public key
 - 1.2.4. Identifies its operational period
 - 1.2.5. Is digitally signed by the issuing CA
- 1.3. “CA” or “Certificate Authority”, means, as defined in the current WBA Certificate Policy, an entity authorized to issue, manage, revoke, and renew Certificates in the Public Key Infrastructure (PKI).
- 1.4. “Certificate Manager” means Sectigo Ltd., or such other entity that creates and issues Certificates.
- 1.5. “RA Agent” means a WBA WRIX Agent as defined in the WBA Certificate Policy.
- 1.6. “WBA Certificate Policy” means the document titled “WRIX PKI Certificate Policy” that the WBA makes publicly available, as amended.

2.0 Certificate Authorization

- 2.1. Upon receipt of a complete and executed Agreement, payment of appropriate fees (see Section 5.0), the Subscriber’s information (see Exhibit A), the Naming Documents (see appropriate Exhibit as described above), and validation of Subscriber’s identity in accordance with the WBA Certificate Policy, Subscriber will receive the Certificates checked above.

3.0 Use of Certificates and Request/Receipt of Certificates

- 3.1. **Adherence to the WBA Certificate Policy.** Subscriber agrees that they will at all times comply with WBA Certificate Policy as may be amended and made available to Subscriber. A Subscriber violation of the WBA Certificate Policy is a breach of this agreement. In the event of a conflict between a term or definition of this agreement and the WInnForum Certificate Policy, the WInnForum Certificate Policy shall govern.
- 3.2. **Embedding and Use of Certificates.** Subscriber shall only embed or otherwise use Certificates as approved in the WBA Certificate Policy. Subscriber shall not embed or otherwise use any Certificate associated with a private key that Subscriber knows or should have known was stolen, intercepted or otherwise compromised in any way. Subscriber shall notify Kyrio promptly at pkiops@kyrio.com in the event a Certificate or CA is lost, stolen or otherwise compromised
- 3.3. **Security of Certificate Private Keys.** Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate. Subscriber shall notify Kyrio promptly at pkiops@kyrio.com in the event a private key is lost, stolen or otherwise compromised.

-
- 3.4. **Prohibited Use.** Pursuant to the WBA Certificate Policy, WBA PKI Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation systems, aircraft communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.
 - 3.5. **No Other Rights.** WBA retains all right, title, and interest in and to its trademarks, the WBA Roots, intermediate certification authorities and Certificates. Kyrio owns and grants no rights, title or interest in any trademark, trade name, service mark, business name or goodwill of Kyrio.

4.0 Term and Termination

- 4.1. **Term.** The term of this Agreement shall begin on the Effective Date and shall continue until the termination occurs as provided herein.
- 4.2. **Termination by Subscriber.** Subscriber may terminate this Agreement, with or without cause, by giving Kyrio sixty days written notice of such termination.
- 4.3. **Termination by Kyrio.** Kyrio may terminate this Agreement for material breach of this Agreement due to Subscriber's negligent action or omission, where such breach is not cured within sixty days of notice to Subscriber; or, where such breach is incapable of cure at the time of the material breach. Examples of breach include but are not limited to: Certificate private keys have been lost, stolen, intercepted or otherwise compromised in any way, a court or governmental agency orders Kyrio or WBA to revoke Subscriber authorization, or, in the case of a CA, failure to provide to Kyrio or pass a WebTrust audit to the WBA Certificate Policy. Kyrio may also terminate this Agreement upon the direction of the WBA. Upon the termination of the Agreement, Kyrio and Subscriber may execute a new Digital Certificate Subscriber Agreement if Subscriber has taken actions to cure the breach and ensure that the breach will not re-occur.
- 4.4. **Termination for Insolvency.** Each party hereto may terminate this Agreement effective immediately upon written notice, should the other party hereto (i) admit in writing its inability to pay its debts generally as they become due; (ii) make a general assignment for the benefit of creditors; (iii) institute proceedings, or have proceedings instituted against it, seeking relief or reorganization under any laws relating to bankruptcy or insolvency; (iv) have a court of competent jurisdiction appoint a receiver, liquidator, or trustee over all or substantially all of such Party's property or provide for the liquidation of such Party's property or business affairs.
- 4.5. **Effect of Termination or Certificate Revocation.** If this Agreement is terminated, or a Certificate is revoked, Subscriber shall discontinue using such Certificate(s) and cease embedding or otherwise using such Certificate(s) in any or all affected client implementations. Subscriber shall keep secret or destroy any unused or revoked Certificates and any associated private keys, and take such other action as is reasonably directed by Kyrio acting on behalf of WBA. Notwithstanding any termination of this Agreement, any un-revoked Certificate(s) used in client implementations that are no longer under the control of Subscriber shall be valid until the expiration of their validity period as stated in the Specifications.

5.0 Fees

- 5.1. **Fees.** Please contact pklops@kyrio.com for fees. Fees are paid in advance of processing of Certificates unless arranged otherwise with Kyrio. Kyrio may, upon thirty (30) days prior notice, modify the Fees with such modification not occurring more than once per calendar year. All payments to Kyrio shall be in U.S. dollars.

-
- 5.2. **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 any other taxes, fees or charges (other than Kyrio or WBA income taxes or other such taxes directly related to their businesses, such as payroll taxes) that may be levied upon either party by taxing authorities other than the United States in connection with this Agreement and shall pay all income taxes that may be levied upon Subscriber.

6.0 Warranty, Indemnity, Limitation of Liability

- 6.1. Subscriber warrants that:
- 6.1.1. The Subscriber shall abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates as described in this agreement and the WBA Certificate Policy; and
 - 6.1.2. each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created; and
 - 6.1.3. Subscriber's private keys are protected from unauthorized use or disclosure; and
 - 6.1.4. all representations made by the Subscriber in this agreement are true; and
 - 6.1.5. all information supplied by the Subscriber and contained in the Certificate is true and does not infringe upon any intellectual property rights; and
 - 6.1.6. the Certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of the WBA Certificate Policy; and
 - 6.1.7. the Subscriber will promptly notify Kyrio upon suspicion of loss or compromise of their private key(s); and
 - 6.1.8. The Subscriber's Certificate shall not contain any trademark infringement.
- 6.2. Kyrio warrants, in compliance with the WBA Certificate Policy, that:
- 6.2.1. Kyrio comply with the stipulations of this WBA Certificate Policy; and
 - 6.2.2. Kyrio comply with and maintains its operations in conformance to the stipulations of the approved Kyrio Certificate Practice Statement; and
 - 6.2.3. There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate; and
 - 6.2.4. There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application
 - 6.2.5. Certificates issued meet all material requirements of the WInnForum Certificate Policy; and
 - 6.2.6. Revocation services (in the event revocation services become applicable) and use of a repository conform to all material requirements of the WInnForum Certificate Policy and the applicable in all material aspects.
- 6.3. **Disclaimer of Warranties. TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE CERTIFICATES, USE OF WHICH IS AUTHORIZED HEREIN, ARE PROVIDED "AS IS" AND KYRIO, CERTIFICATE MANAGER, AND WINNFORUM DISCLAIM ALL REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUIET ENJOYMENT, ACCURACY, SECURITY, OR NON-INFRINGEMENT.**

-
- 6.4. **Indemnification.** Subscriber shall indemnify and hold harmless Kyrio, WBA, the Certificate Manager and their respective, directors, employees, and agents, for any claim arising from or related to:
- 6.4.1. Falsehood or misrepresentation of fact by the Subscriber in obtaining Certificates; and
 - 6.4.2. failure by the Subscriber to disclose a material fact in this agreement, if the misrepresentation or omission was made negligently or with intent to deceive any party; and
 - 6.4.3. Subscriber's failure to take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key(s); and
 - 6.4.4. Subscriber's use of a name (including that infringes upon the Intellectual Property Rights) of a third party.
 - 6.4.5. Such indemnification obligations shall be subject to: (i) Kyrio, WBA, and/or the Certificate Manager notifying Subscriber, in writing of any such claim and (ii) Subscriber having the sole control of the defense and all negotiations for any settlement or compromise of such claim, provided, however, that Kyrio, WBA, and/or the Certificate Manager may participate in such defense using counsel of its own choice and at its sole expense.
- 6.5. **Limitation of Liability. TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL 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 CLIENT IMPLEMENTATIONS, WHETHER DAMAGES OF THIS NATURE WERE FORESEEABLE OR NOT, AND EVEN IF THAT PARTY HAD BEEN ADVISED THAT DAMAGES OF THIS NATURE WERE POSSIBLE. IN NO EVENT SHALL EITHER PARTY BE LIABLE UNDER THIS AGREEMENT TO THE OTHER PARTY FOR ANY AMOUNT EXCEEDING THE FEES ACTUALLY RECEIVED BY KYRIO FROM SUBSCRIBER IN PERFORMANCE OF THIS AGREEMENT. ANY DAMAGES ARISING FROM OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED THE AMOUNT SUBSCRIBER HAS PAID FOR DIGITAL CERTIFICATES AND/OR CERTIFICATE AUTHORTIES IN THE YEAR PRIOR TO THE DATE OF A FILED CLAIM.**
- 6.6. **Subscriber Liability for Subscriber Supplied Information.** Subscriber is solely liable for the resulting 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 Certificates which may require Subscriber to purchase additional Certificates.

7.0 **General**

- 7.1. **Notices.** Any notices, required or permitted to be made or given to either party pursuant to this Agreement shall be in writing and shall be delivered to the email address, sent with confirmation receipt, set forth on the first page or in Exhibit A, or to such other address as the receiving party may have designated by written notice given to the other party. Legal notices shall be sent to the person listed as the Legal Contact. Technical notices shall be sent to the name listed as the Technical Contact. Operational notices to Kyrio shall be pklops@kyrio.com. Legal notices shall be sent to legal@kyrio.com.
- 7.2. **Insurance.** Subscriber shall maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.
- 7.3. **Export.** The export of commodities or technical data from the United States of America and/or the re-export from foreign countries of commodities or technical data or devices of United States of America

origin, may be conditioned upon the issuance of an export license by the government of the United States of America. You represent that you will not export or re-export any commodities, technical data or direct devices of technical data in furtherance of unless and until you have complied in all respects with the United States of America Export Control Regulations. You shall indemnify and hold Kyrio and its parent company, CableLabs, harmless for any violation of the export control laws.

- 7.4. **Audit.** Kyrio or its duly authorized representatives shall be permitted, upon reasonable notice, and subject to appropriate non-disclosure terms, to inspect all records pertaining to the Certificates, including, without limitation, records related or pertaining to the security, usage, revocation, and distribution of the Certificates. The inspections may be made notwithstanding termination of this Agreement while any outstanding claim remains unsettled in the view of either party. In the event Kyrio needs to conduct an audit due to a discrepancy discovered in a prior audit, Subscriber shall be responsible for its own expenses incurred for such subsequent audit.
- 7.5. **Irreparable Harm.** Subscriber and Kyrio acknowledge and agree that due to the unique and sensitive nature of the use of the Certificates and Certificate Authorities authorized herein, including any private keys therein, there can be no adequate remedy at law for breach of Subscriber's obligations hereunder, that such breach or unauthorized use or release of the Certificates will cause material damage and result in irreparable harm. Therefore, upon any such breach or any threat thereof, Kyrio shall be entitled to appropriate equitable relief in addition to whatever remedies it might have at law.
- 7.6. **Waiver.** Any waiver by either party hereto of any breach of this Agreement shall not constitute a waiver of any subsequent or other breach.
- 7.7. **Survival.** Sections 3.0, 4.5, 6.0, 6.4, 6.5, 6.6, 7.3, 7.4, 7.7, and 7.9 shall survive any termination of the Agreement.
- 7.8. **Assignment.** Subscriber may not assign this Agreement without the express, prior written approval of Kyrio.
- 7.9. **Third Party Beneficiaries.** WBA and the Certificate Manager are the sole third-party beneficiaries of this Agreement.
- 7.10. **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.
- 7.11. **Governing Law; Forum.** This Agreement shall be construed in accordance with the law of the state of Colorado, without regard to its conflict of laws rules. The Parties hereby agree to exclusive jurisdiction and venue in the federal/state courts located in the city and county of Denver. The language of this agreement is English. The following applies in the appropriate jurisdictions: Les parties aux présentes ont exigé que cette entente et tous autres documents qui y sont reliés par les présentes soient rédigés en anglais.

EXHIBIT A
SUBSCRIBER'S INFORMATION

Notes:

- 1) Fields marked with (*) are compulsory for the specified section.
- 2) When entering phone or fax numbers ensure that you **include country and area codes**.
- 3) **Organization name** is a compulsory field and it is recommended it be the **legally registered business name**.
 - a. Use of special characters such as () & * % \$ # @ ! + = ^ is not permitted.

CORPORATE INFORMATION:

Organization Name*: (Full Legal Name)
Legal Headquarters Address*: (City, State or Province, Zip/Postal Code, Country)
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 person must work for the organization requesting this service and is an authorized representative of the organization. This individual will authorize the other account contacts including administrators who will request Certificates from Kyrio. This person may periodically receive email regarding issues or events occurring with this service.

Subscriber Name*:	
Title*:	E-mail*:
Phone*:	Fax:

PRIMARY ADMINISTRATOR CONTACT:

This is the person who is authorized to request and receive certificates. An administrator certificate will be delivered to this person at this address. This will generally be the manufacturing location where production certificates are installed.

Same as the Corporate Contact? YES NO

Primary Administrator Contact*:	
Title*:	E-mail*:
Phone*:	Fax:
Address*:	City and State*:
Zip/Postal Code*:	Country*:

SECOND ADMINISTRATOR CONTACT:

This person is authorized to back up the primary administrator contact. They are also authorized to request and receive certificates. An administrator certificate will be delivered to this person at this address. This will generally be the manufacturing location where production certificates are installed.

Second Administrator Contact*:	
Title*:	E-mail*:
Phone*:	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 the PKI with Kyrio.

Technical Contact*:	
Title*:	E-mail*:
Phone*:	Fax:

SUBSCRIBER'S LEGAL CONTACT

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

Legal Contact*:	
Title*:	E-mail*:
Phone*:	Fax:
Address*:	City and State*:
Zip/Postal Code*:	Country*:

SUBSCRIBER'S BILLING CONTACT:

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

Billing Contact*:	
Title*:	E-mail*:
Phone*:	Fax:
Address*:	City and State*:
Zip/Postal Code*:	Country*:

EXHIBIT B
WBA WRIX ECC End-Entity Server-Client Naming Application

Organization Name:	
Date of Application (MM/DD/YYYY):	
Contact Name:	Phone:
Contact E-mail:	

Key Details

Public Key Algorithm	EC
Public Key Size	P-384 (secp384r1)

Certificate Details

Version	v3		
Serial number	Unique Positive Integer assigned by the CA		
		Internal Use	
Subject DN	c= o= ou=WBA:WRIX End-Entity cn= uid=	FROM ORG FROM ORG FIXED FROM UPLOAD FROM ORG	
Issuer DN	c=US o=Kyrio, Inc. ou=WBA cn=openroaming.org dnq=WBA WRIX ECC Intermediate CA-2		
notBefore	<Issuing Date>		
notAfter	<Issuing Date> + 3 years		
Signature Hashing Algorithm	<input type="checkbox"/> SHA-256	<input checked="" type="checkbox"/> SHA-384	<input type="checkbox"/> SHA-512

Certificate Extensions

Extension Identifier	OID	Critical	Value
keyUsage	{id-ce 15}	TRUE	
digitalSignature			SET (1)
keyAgreement			SET (1)
subjectKeyIdentifier	{id-ce 14}	FALSE	
keyIdentifier			<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>
authorityKeyIdentifier	{id-ce 35}	FALSE	
keyIdentifier			<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>
subjectAltName	{id-ce 17}	FALSE	
dNSName			(multiple) Internal Use: FROM UPLOAD REQUIRED
iPAddress			(multiple) FROM UPLOAD
rfc822Name			(multiple) FROM UPLOAD
certificatePolicies	{id-ce 32}	FALSE	
certPolicyId			SET 1.3.6.1.4.1.14122.1.1.6
extKeyUsage	{id-ce 37}	FALSE	
keyPurposeID			
id-kp-clientAuth			SET (1)
id-kp-serverAuth			SET (1)
cRLDistributionPoint	{id-ce 31}	FALSE	
distributionPoint			<HTTP URL for DER CRL>
authorityInfoAccess	{id-pe 1}	FALSE	
accessDescription			
accessMethod			OCSP
accessLocation			<HTTP URL for OCSP Responder>

Approval

Date

Corporate Contact: _____

EXHIBIT C

WBA WRIX ECC End-Entity Server Only Naming Application

Organization Name:	
Date of Application (MM/DD/YYYY):	
Contact Name:	Phone:
Contact E-mail:	

Key Details

Public Key Algorithm	EC
Public Key Size	P-384 (secp384r1)

Certificate Details

Version	v3		
Serial number	Unique Positive Integer assigned by the CA		
		Internal Use	
Subject DN	c= o= ou=WBA:WRIX End-Entity cn= uid=	FROM ORG FROM ORG FIXED FROM UPLOAD FROM ORG	
Issuer DN	c=US o=Kyrio, Inc. ou=WBA cn=openroaming.org dnq=WBA WRIX ECC Intermediate CA-2		
notBefore	<Issuing Date>		
notAfter	<Issuing Date> + 3 years		
Signature Hashing Algorithm	<input type="checkbox"/> SHA-256	<input checked="" type="checkbox"/> SHA-384	<input type="checkbox"/> SHA-512

Certificate Extensions

Extension Identifier	OID	Critical	Value
keyUsage	{id-ce 15}	TRUE	
digitalSignature			SET (1)
keyAgreement			SET (1)
subjectKeyIdentifier	{id-ce 14}	FALSE	
keyIdentifier			<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>
authorityKeyIdentifier	{id-ce 35}	FALSE	
keyIdentifier			<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>
subjectAltName	{id-ce 17}	FALSE	
dNSName			(multiple) Internal Use: FROM UPLOAD REQUIRED
iPAddress			(multiple) FROM UPLOAD
rfc822Name			(multiple) FROM UPLOAD
certificatePolicies	{id-ce 32}	FALSE	
certPolicyId			SET 1.3.6.1.4.1.14122.1.1.6
extKeyUsage	{id-ce 37}	FALSE	
keyPurposeID			
id-kp-serverAuth			SET (1)
cRLDistributionPoint	{id-ce 31}	FALSE	
distributionPoint			<HTTP URL for DER CRL>
authorityInfoAccess	{id-pe 1}	FALSE	
accessDescription			
accessMethod			OCSP
accessLocation			<HTTP URL for OCSP Responder>

Approval

Date

Corporate Contact: _____

EXHIBIT D
WBA WRIX ECC End-Entity Client Only Naming Application

Organization Name:	
Date of Application (MM/DD/YYYY):	
Contact Name:	Phone:
Contact E-mail:	

Key Details

Public Key Algorithm	EC
Public Key Size	P-384 (secp384r1)

Certificate Details

Version	v3		
Serial number	Unique Positive Integer assigned by the CA		
		Internal Use	
Subject DN	c= o= ou=WBA:WRIX End-Entity cn= uid=	FROM ORG FROM ORG FIXED FROM UPLOAD FROM ORG	
Issuer DN	c=US o=Kyrio, Inc. ou=WBA cn=openroaming.org dnq=WBA WRIX ECC Intermediate CA-2		
notBefore	<Issuing Date>		
notAfter	<Issuing Date> + 3 years		
Signature Hashing Algorithm	<input type="checkbox"/> SHA-256	<input checked="" type="checkbox"/> SHA-384	<input type="checkbox"/> SHA-512

Certificate Extensions

Extension Identifier	OID	Critical	Value
keyUsage	{id-ce 15}	TRUE	
digitalSignature			SET (1)
keyAgreement			SET (1)
subjectKeyIdentifier	{id-ce 14}	FALSE	
keyIdentifier			<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>
authorityKeyIdentifier	{id-ce 35}	FALSE	
keyIdentifier			<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>
subjectAltName	{id-ce 17}	FALSE	
dNSName			(multiple) Internal Use: FROM UPLOAD
iPAddress			(multiple) FROM UPLOAD
rfc822Name			(multiple) FROM UPLOAD
certificatePolicies	{id-ce 32}	FALSE	
certPolicyId			SET 1.3.6.1.4.1.14122.1.1.6
extKeyUsage	{id-ce 37}	FALSE	
keyPurposeID			
id-kp-clientAuth			SET (1)
cRLDistributionPoint	{id-ce 31}	FALSE	
distributionPoint			<HTTP URL for DER CRL>
authorityInfoAccess	{id-pe 1}	FALSE	
accessDescription			
accessMethod			OCSP
accessLocation			<HTTP URL for OCSP Responder>

Approval

Date

Corporate Contact: _____

EXHIBIT E
WBA WRIX ECC End-Entity RA Agent Naming Application

Organization Name:	
Date of Application (MM/DD/YYYY):	
Contact Name:	Phone:
Contact E-mail:	

Key Details

Public Key Algorithm	EC
Public Key Size	P-384 (secp384r1)

Certificate Details

Version	v3		
Serial number	Unique Positive Integer assigned by the CA		
		Internal Use	
Subject DN	c= o= ou=WBA:WRIX RA cn= uid=	FROM UPLOAD FROM UPLOAD FIXED FROM UPLOAD FROM UPLOAD	
Issuer DN	c=US o=Kyrio, Inc. ou=WBA cn=openroaming.org dnq=WBA WRIX ECC Intermediate CA-2		
notBefore	<Issuing Date>		
notAfter	<Issuing Date> + 3 years		
Signature Hashing Algorithm	<input type="checkbox"/> SHA-256	<input checked="" type="checkbox"/> SHA-384	<input type="checkbox"/> SHA-512

Certificate Extensions

Extension Identifier	OID	Critical	Value
keyUsage	{id-ce 15}	TRUE	
digitalSignature			SET (1)
keyAgreement			SET (1)
subjectKeyIdentifier	{id-ce 14}	FALSE	
keyIdentifier			<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>
authorityKeyIdentifier	{id-ce 35}	FALSE	
keyIdentifier			<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>
subjectAltName	{id-ce 17}	FALSE	
rfc822Name			(multiple) Internal Use: FROM UPLOAD
certificatePolicies	{id-ce 32}	FALSE	
certPolicyId			SET 1.3.6.1.4.1.14122.1.1.6
extKeyUsage	{id-ce 37}	FALSE	
keyPurposeID			
id-kp-clientAuth			SET (1)
cRLDistributionPoint	{id-ce 31}	FALSE	
distributionPoint			<HTTP URL for DER CRL>
authorityInfoAccess	{id-pe 1}	FALSE	
accessDescription			
accessMethod			OCSP
wbaRegAuth	{1.3.6.1.4.1.14122.1.2.1}	FALSE	
registrationAuthority			Set (1) [BOOLEAN]

Approval

Date

Corporate Contact: _____

EXHIBIT F
WBA WRIX ECC End-Entity TRIAL Server-Client Naming Application

Organization Name:	
Date of Application (MM/DD/YYYY):	
Contact Name:	Phone:
Contact E-mail:	

Key Details

Public Key Algorithm	EC
Public Key Size	P-384 (secp384r1)

Certificate Details

Version	v3		
Serial number	Unique Positive Integer assigned by the CA		
		Internal Use	
Subject DN	c= o= ou=WBA:WRIX End-Entity cn= uid=	FROM ORG FROM ORG FIXED FROM UPLOAD FROM ORG	
Issuer DN	c=US o=Kyrio, Inc. ou=WBA cn=openroaming.org dnq=WBA WRIX ECC Intermediate CA-2		
notBefore	<Issuing Date>		
notAfter	<Issuing Date> + 120 days		
Signature Hashing Algorithm	<input type="checkbox"/> SHA-256	<input checked="" type="checkbox"/> SHA-384	<input type="checkbox"/> SHA-512

Certificate Extensions

Extension Identifier	OID	Critical	Value	
keyUsage	{id-ce 15}	TRUE		
digitalSignature			SET (1)	
keyAgreement			SET (1)	
subjectKeyIdentifier	{id-ce 14}	FALSE		
keyIdentifier			<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>	
authorityKeyIdentifier	{id-ce 35}	FALSE		
keyIdentifier			<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>	
subjectAltName	{id-ce 17}	FALSE		Internal Use:
dNSName			(multiple)	FROM UPLOAD REQUIRED
iPAddress			(multiple)	FROM UPLOAD
rfc822Name			(multiple)	FROM UPLOAD
certificatePolicies	{id-ce 32}	FALSE		
certPolicyId			SET 1.3.6.1.4.1.14122.1.1.6	
extKeyUsage	{id-ce 37}	FALSE		
keyPurposeID				
id-kp-clientAuth			SET (1)	
id-kp-serverAuth			SET (1)	
cRLDistributionPoint	{id-ce 31}	FALSE		
distributionPoint			<HTTP URL for DER CRL>	
authorityInfoAccess	{id-pe 1}	FALSE		
accessDescription				
accessMethod			OCSP	
accessLocation			<HTTP URL for OCSP Responder>	

Approval

Date

Corporate Contact: _____

EXHIBIT G
WBA WRIX ECC End-Entity TRIAL Server Only Naming Application

Organization Name:	
Date of Application (MM/DD/YYYY):	
Contact Name:	Phone:
Contact E-mail:	

Key Details

Public Key Algorithm	EC
Public Key Size	P-384 (secp384r1)

Certificate Details

Version	v3		
Serial number	Unique Positive Integer assigned by the CA		
			Internal Use
Subject DN	c= o= ou=WBA:WRIX End-Entity cn= uid=	FROM ORG FROM ORG FIXED FROM UPLOAD FROM ORG	
Issuer DN	c=US o=Kyrio, Inc. ou=WBA cn=openroaming.org dnq=WBA WRIX ECC Intermediate CA-2		
notBefore	<Issuing Date>		
notAfter	<Issuing Date> + 120 days		
Signature Hashing Algorithm	<input type="checkbox"/> SHA-256	<input checked="" type="checkbox"/> SHA-384	<input type="checkbox"/> SHA-512

Certificate Extensions

Extension Identifier	OID	Critical	Value	
keyUsage	{id-ce 15}	TRUE		
digitalSignature			SET (1)	
keyAgreement			SET (1)	
subjectKeyIdentifier	{id-ce 14}	FALSE		
keyIdentifier			<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>	
authorityKeyIdentifier	{id-ce 35}	FALSE		
keyIdentifier			<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>	
subjectAltName	{id-ce 17}	FALSE		Internal Use:
dNSName			(multiple)	FROM UPLOAD REQUIRED
iPAddress			(multiple)	FROM UPLOAD
rfc822Name			(multiple)	FROM UPLOAD
certificatePolicies	{id-ce 32}	FALSE		
certPolicyId			SET 1.3.6.1.4.1.14122.1.1.6	
extKeyUsage	{id-ce 37}	FALSE		
keyPurposeID				
id-kp-serverAuth			SET (1)	
cRLDistributionPoint	{id-ce 31}	FALSE		
distributionPoint			<HTTP URL for DER CRL>	
authorityInfoAccess	{id-pe 1}	FALSE		
accessDescription				
accessMethod			OCSP	
accessLocation			<HTTP URL for OCSP Responder>	

Approval

Date

Corporate Contact: _____

EXHIBIT H
WBA WRIX ECC End-Entity TRIAL Client Only Naming Application

Organization Name:	
Date of Application (MM/DD/YYYY):	
Contact Name:	Phone:
Contact E-mail:	

Key Details

Public Key Algorithm	EC
Public Key Size	P-384 (secp384r1)

Certificate Details

Version	v3		
Serial number	Unique Positive Integer assigned by the CA		
		Internal Use	
Subject DN	c= o= ou=WBA:WRIX End-Entity cn= uid=	FROM ORG FROM ORG FIXED FROM UPLOAD FROM ORG	
Issuer DN	c=US o=Kyrio, Inc. ou=WBA cn=openroaming.org dnq=WBA WRIX ECC Intermediate CA-2		
notBefore	<Issuing Date>		
notAfter	<Issuing Date> + 120 days		
Signature Hashing Algorithm	<input type="checkbox"/> SHA-256	<input checked="" type="checkbox"/> SHA-384	<input type="checkbox"/> SHA-512

Certificate Extensions

Extension Identifier	OID	Critical	Value	
keyUsage	{id-ce 15}	TRUE		
digitalSignature			SET (1)	
keyAgreement			SET (1)	
subjectKeyIdentifier	{id-ce 14}	FALSE		
keyIdentifier			<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>	
authorityKeyIdentifier	{id-ce 35}	FALSE		
keyIdentifier			<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>	
subjectAltName	{id-ce 17}	FALSE		Internal Use:
dNSName			(multiple)	FROM UPLOAD
iPAddress			(multiple)	FROM UPLOAD
rfc822Name			(multiple)	FROM UPLOAD
certificatePolicies	{id-ce 32}	FALSE		
certPolicyId			SET 1.3.6.1.4.1.14122.1.1.6	
extKeyUsage	{id-ce 37}	FALSE		
keyPurposeID				
id-kp-clientAuth			SET (1)	
cRLDistributionPoint	{id-ce 31}	FALSE		
distributionPoint			<HTTP URL for DER CRL>	
authorityInfoAccess	{id-pe 1}	FALSE		
accessDescription				
accessMethod			OCSP	
accessLocation			<HTTP URL for OCSP Responder>	

Approval

Date

Corporate Contact: _____