WIRELESS POWER CONSORTIUM, INC. AUTHORIZED MANUFACTURER AGREEMENT

This Authorized Manufacturer Agreement (the "Agreement") is made by and between Wireless Power Consortium, Inc. ("WPC") and _____(the "Manufacturer"), having its registered office at _____, and is effective as of _____(the "Effective Date").

Whereas WPC has created one or more public key cryptography-based systems for validating whether particular interoperable wireless power transfer products comply with its wireless power specifications, to the benefit of consumers and industry alike;

Whereas Manufacturer wishes to participate in this system by:

- Obtaining Secure Storage Subsystems;
- Appointing a Manufacturer CA Service Provider to create a Manufacturer CA Certificate on its behalf;
- Directing the MCSP to provision such Secure Storage Subsystems by cryptographically signing Product Unit Certificates, using the public key associated with this Manufacturer CA Certificate; and
- Incorporating these Provisioned Secure Storage Subsystems into Manufacturer's Certified Products.

Whereas WPC is willing to authorize Manufacturer to participate in its cryptography-based authentication system in accordance with the provisions of this Agreement;

In consideration of the mutual covenants and obligations set forth herein, the parties hereto agree as follows:

1 Definitions

1.1 "Affiliate" means, with respect to Manufacturer, a legal entity directly or indirectly in Control of, Controlled by, or under common Control with Manufacturer, for so long as such Control exists. For purposes of the foregoing, "Control" and its derivatives means the legal, beneficial, or equitable ownership, directly or indirectly, of more than 50% of the capital stock (or other ownership interest, if not a corporation) of such entity ordinarily having voting rights.

1.2 "Authentication Specification" means the part of the applicable WPC Specification (as defined in WPC's Trademark License Policy) titled "Authentication Protocol" for each WPC Specification, as such protocol may be updated from time to time, plus all related supporting documents.

1.3 "Authorized Manufacturer" means an entity that has been expressly designated as an authorized manufacturer by WPC pursuant to WPC's Authorized Manufacturer Agreement, without such designation having been withdrawn or revoked.

1.4 "Certified Product" has the meaning set forth in WPC's Product Certification Process Document.

1.5 "Hardware Security Module" means a dedicated physical computing device that safeguards and

manages cryptographic keys and provides cryptographic processing.

1.6 "Manufacturer CA Service Provider" or "MCSP" means an entity that has been expressly designated as a MCSP by WPC pursuant to WPC's Manufacturer Certification Authority Agreement, without such designation having been withdrawn or revoked.

1.7 "Manufacturer CA Certificate" means an electronic document in a format specified by the WPC that identifies the public key of a public-private key pair used by a MCSP, and carries a digital signature that can be cryptographically validated with the public key of a WPC Root CA.

1.8 "Material Breach" means any substantial breach of this Agreement by a party that is not cured within thirty (30) days of written notice by the non-breaching party of such breach. Any related series of substantial breaches shall be deemed a single Material Breach. A substantial breach that is incapable of cure (such as the unauthorized disclosure of a private cryptographic key) will be deemed a Material Breach upon notice by the non-breaching party.

1.9 "Product Unit Certificate" means an electronic document in a format specified by the WPC that identifies the public key of a public-private key pair used by a particular product instance, and carries a digital signature that can be cryptographically validated with the public key in a Manufacturer CA Certificate.

1.10 "Provisioned Secure Storage Subsystem" means a Secure Storage Subsystem that has been provisioned (i.e., a MCSP has created a Product Unit Certificate for the public key corresponding to the private key stored within the Provisioned Secure Storage Subsystem).

1.11 "Root Certification Authority" or "Root CA" means an entity designated by WPC from time to time whose public key serves as the most trusted datum (i.e. the beginning of trust paths) to validate Manufacturer CA Certificates for a WPC public key infrastructure (PKI).

1.12 "Secure Storage Subsystem" means a tamper resistant subsystem that protects one or more cryptographic key values against exposure outside that subsystem.

1.13 "Test Platform" has the meaning set forth in WPC's Product Certification Process Document.

1.14 "WPC ID" has the meaning set forth in WPC's Product Certification Process Document.

1.15 Other defined terms. Any capitalized terms not defined in this Agreement shall have the meaning described in the applicable WPC Specification, WPC's Product Certification Process Document, or WPC's Product Certification Policy.

2 Authorization

2.1 Subject to the terms and conditions of this Agreement, including (without limitation) meeting the obligations set forth in Section 3 and payment of applicable fees, WPC hereby authorizes Manufacturer to:

(a) Engage one or more MCSPs to generate a cryptographic key pair on behalf of Manufacturer, and arrange for the public key associated with such a key pair to be cryptographically signed by the Root CA designated by WPC, resulting in a Manufacturer CA Certificate for Manufacturer;

(b) Direct MCSPs to provision Secure Storage Subsystems by cryptographically signing Product Unit Certificates, using the public key associated with its Manufacturer CA Certificate;

(c) Incorporate the Provisioned Secure Storage Subsystems into Manufacturer's Certified Products, identified by the WPC ID included in the Product Unit Certificate.

2.2 Manufacturer is permitted to also enter into a Manufacturer CA Agreement, provided that it meets all applicable criteria associated with that role. In such a case the Manufacturer will be receiving and providing the services described in this Agreement on its own behalf. The Manufacturer may also contract with one or more unrelated MCSPs, in its discretion. If Manufacturer contracts with more than one MCSP, each MCSP will generate unique cryptographic key pairs for Manufacturer, so Manufacturer may have multiple Manufacturer Certificates created on its behalf. Any contractual or other business arrangements between a Manufacturer and a MCSP must not conflict with this Agreement, but otherwise the Manufacturer and the MCSP are free to structure their relationship as they choose, in their discretion.

3 Obligations

3.1 In connection with WPC's authentication processes, Manufacturer shall perform only those activities expressly authorized by this Agreement. Without limiting any other term of this Agreement, all activities authorized by this Agreement shall be performed by the Manufacturer in accordance with the standard of care and diligence normally practiced by industry professionals highly skilled in implementations of cryptography-based security.

3.2 Manufacturer shall meet the requirements detailed in the relevant Authentication Specification in connection with its products that implement such specification.

3.3 Manufacturer shall meet the requirements for secure storage and handling of secrets detailed in Annex A, Section 2. The information provided in Sections 1 and 3 of Annex A is provided on an informational basis only, to indicate the terms WPC intends to impose on MCSPs under separate contracts, and does not create any obligation on the part of Manufacturer.

3.4 Manufacturer acknowledges that WPC has the right to revoke certificates in accordance with Annex B.

3.5 Upon reasonable request from WPC, Manufacturer shall enable a WPC representative to inspect or audit its performance under this Agreement, as described in Annex C.

3.6 Manufacturer shall pay the fees described in Annex D.

3.7 WPC shall be entitled to make updates to Annexes A, B, C, and D as follows:

(a) In advance of any updates to any Annexes, WPC will provide Manufacturer the opportunity to review proposed updates and provide inputs, but WPC will retain discretion over the final content of any updates;

(b) WPC may provide updated versions of Annexes A, B, or C via written notice, and the updated versions will be effective and deemed incorporated into this Agreement ninety (90) days after such written notice.

(c) WPC may provide an updated version of Annex D via written notice, and the updated version will be effective and deemed incorporated into this Agreement sixty (60) days after such written notice.

3.8 Manufacturer shall maintain its membership in WPC in good standing during the term of this Agreement.

4 Term and Termination

4.1 This Agreement shall enter into force on the Effective Date and shall continue for an initial term of two (2) years. The Agreement shall be automatically extended for additional one (1) year terms, unless the terminating party gives written notice of termination no later than ninety (90) days prior to the expiry of the then current term.

4.2 This Agreement will terminate immediately if Manufacturer ceases to be a member of WPC. Either party may terminate this Agreement immediately in the event of a Material Breach by the other party. Such right of termination shall not be exclusive of any other remedy or means of redress to which the non-defaulting party may be lawfully entitled, and all such remedies shall be cumulative.

4.3 Manufacturer will use best efforts to notify any MCSP that it receives services from related to this Agreement of any anticipated termination promptly upon its knowledge or awareness, and to cooperate in good faith with these MCSPs and WPC to appropriately manage authentication processes associated with deployed Manufacturer products post-termination.

4.4 Sections 1, 3.1 – 3.6, 4, 5 and 6 shall survive expiration or termination of this Agreement. In addition, any other provisions that by their terms are intended to survive expiration or termination of this Agreement shall survive.

4.5 Effect of Termination. Upon termination of this Agreement, Manufacturer will immediately cease all of the activities authorized under Section 2. Manufacturer will have a period not to exceed ninety days to use any existing Provisioned Secure Storage Subsystems in its possession.

5 Remedies

5.1 Manufacturer acknowledges and agrees that, due to the potential for lasting effect and harm that would result from a Material Breach of this Agreement, if Manufacturer commits a Material Breach of its obligations hereunder, monetary damages alone may not be a sufficient remedy. Accordingly, WPC shall have the right to seek an injunction to prevent or restrain any Material Breach, without prejudice to its right to terminate this Agreement for reason of such Material Breach. The rights to seek injunctive relief and terminate this Agreement are cumulative and not exclusive of any other rights that might be available to WPC under this Agreement or at law.

5.2 For avoidance of doubt, the parties agree that the following actions would cause lasting effect and serious harm:

(a) Enabling any third party (other than contractors acting on Manufacturer's behalf in accordance with this Agreement) to use a Provisioned Secure Storage Subsystem in a product;

(b) Using a Product Unit Certificate or a Provisioned Secure Storage Subsystem in any product other than the product specifically identified by the WPC ID included in the associated Product Unit Certificate;

(c) If known to the Manufacturer, disclosing the private key associated with a Provisioned Secure Storage Subsystem to any third party, unless expressly authorized by WPC.

5.3 For avoidance of doubt, and without limiting Section 5.1 or any other term of this Agreement, the parties agree the actions identified in Section 5.2 shall be Material Breaches if performed knowingly by Manufacturer.

6 General

6.1 No party hereto grants or receives, by implication, estoppel, or otherwise, any right under any patent, trademark, copyright or any other intellectual property right in connection with this Agreement.

6.2 No failure or delay by either party to enforce any of its rights under this Agreement will operate as a waiver of such right.

6.3 No party hereto makes any implied warranties under this Agreement. Without limiting any obligation of the Manufacturer described in Section 3, all materials and information exchanged between the parties are provided "AS IS" with no warranties whatsoever, whether express, implied or statutory, including, but not limited to any warranty of merchantability, non-infringement, fitness for any particular purpose, or any warranty otherwise arising out of any proposal, specification, guide, design or sample.

6.4 In no event will WPC or Manufacturer be liable to each other for any loss of profits, incidental, consequential, indirect, or special damages arising out of, or related to, this Agreement, even when such party had advance notice of the possibility of such damages.

6.5 Manufacturer agrees to indemnify, defend, and hold harmless WPC as well as its officers, directors, employees, and agents for, from, and against any and all third party claims, third party demands, losses, liabilities, fines, sanctions, judgments, awards, costs, and expenses (including reasonable attorneys' fees and costs) incurred by WPC through a claim or allegation arising out of or caused by: (i) a Material Breach by Manufacturer of this Agreement; (ii) Manufacturer adding or attempting to add WPC to a lawsuit between Manufacturer and a MCSP; or (iii) Manufacturer's false or misleading description of fact, or false or misleading representation of fact, in connection with the marketing, advertising, promotion, endorsement, sale, or distribution of its products or services; provided, however, that in no case shall Manufacturer be required to indemnify WPC regarding a claim or allegation that arises from the inaccuracy of any information provided by WPC. Manufacturer shall not enter into any settlement that requires any obligation, financial or otherwise, of WPC, without WPC's prior written consent, which consent shall not be unreasonably withheld.

6.6 This Agreement shall be construed under and governed by the laws of the United States and the State of New York, USA, without reference to conflict-of-laws principles.

6.7 The Manufacturer and WPC are independent companies and nothing in this Agreement shall be construed as a partnership or joint venture between the parties.

6.8 This Agreement sets forth the entire understanding of the parties with respect to the subject matter hereof, and supersedes all prior agreements and understandings relating hereto. No modifications or additions to or deletions from this Agreement, or waiver of any right hereunder, shall be binding unless accepted in writing by an authorized representative of each party.

6.9 The exercise by any party of any remedy under this Agreement will be without prejudice to its other remedies under this Agreement or at law.

6.10 Upon providing reasonably advanced written notice to Manufacturer, WPC may assign its rights and obligations under this Agreement to a successor in interest. WPC shall consider in good faith any reasonable objection Manufacturer may have to the assignment of the Agreement by WPC (e.g., proposed assignment in conflict with applicable laws; proposed assignment to a competitor of Manufacturer, etc.). Manufacturer may not assign any rights or obligations under this Agreement without WPC's prior written consent which shall not be unreasonably withheld.

6.11 Section headings in this Agreement are for convenience only and shall not affect the interpretation of any provision of this Agreement. All references to section numbers in this Agreement shall refer to sections of this Agreement unless explicitly stated otherwise.

6.12 Nothing in this Agreement shall prohibit or restrict Manufacturer from independently developing competing technologies and standards or to license its patent rights to third parties, including without limitation, to enable competing technologies and standards.

6.13 Any notice under this Agreement shall be sent to:

If to WPC:

Wireless Power Consortium, Inc.
attn.: Executive Director
4315 50th Street NW
Suite 100 # 7344
Washington, DC 20016, USA
tel. +1 202 933 5055
e-mail: administrator@wirelesspowerconsortium.com

If to Manufacturer:

Name of contact person or department: _____

Address: _____

_____

_____

Tel: _____

E-mail: _____

The primary Manufacturer contact for technical and operational matters in connection with this Agreement will be:

Name of contact person or department: _____

Address: _____

_____

_____

Tel: _____

E-mail: _____

6.14 Manufacturer may exercise its rights and perform its obligations under this Agreement via its Affiliates, provided that (i) Manufacturer shall ensure that such Affiliates comply with the terms of this Agreement and (ii) Manufacturer shall be responsible for any breach of such terms by such Affiliated Entities as if such breach had been by Manufacturer.

[signature page follows]

As witness, Manufacturer and WPC have, through their duly authorised representatives, executed this Agreement to be effective as of the Effective Date.

Manufacturer	Wireless Power Consortium, Inc.
Company name: _____ _____ _____	
Signature: _____	Signature: _____
Name: _____	Name: Paul Struhsaker
Title: _____	Executive Director

ANNEX A:
Requirements for secure storage and handling of secrets

1 Requirements for Manufacturer CA Service Provider

1.1 General

- An MCSP may issue Product Unit Certificates to Authorized Manufacturers.
- MCSP shall cease issuing Product Unit Certificates to a company when given notice by WPC that this company's Manufacturer Agreement with the WPC has terminated.

1.2 Requirements for Manufacturer CA Certificates

- MCSP shall obtain a unique Manufacturer CA Certificate for each Authorized Manufacturer that it serves.
- Private keys related to a Manufacturer CA Certificate shall be protected by a hardware security module (HSM), certified at least to FIPS-140-2 Level 3, or CC EAL4+ (EAL4 augmented by ALC_DVS.2) or higher. The HSM shall be operated in a secure environment with related security process for the provisioning ensuring the correct handling of the HSM.
- MCSP shall generate a unique public-private key pair for each certificate signing request for a Manufacturer CA Certificate.

1.3 Requirements for Product Unit Certificates

- MCSP must not include a WPC ID in a Product Unit Certificate for an Authorized Manufacturer unless the MCSP has verified that such WPC ID has been assigned to this Authorized Manufacturer by the WPC. The WPC shall provide MCSP with a method to verify the assignment of WPC IDs [in the MCSP user guide].

1.4 Requirements for Provisioning Secure Storage Subsystems

Provisioning is the process of creating a Product Unit Certificate that matches the private key in a Secure Storage Subsystem.

- MCSP shall ensure that Provisioned Secure Storage Subsystems it supplies to an Authorized Manufacturer comply with the requirement for Provisioned Secure Storage Subsystems (Section 3 of this Annex).
- MCSP may not provision Secure Storage Subsystems that were supplied by a 3rd party by issuing Product Unit Certificates for their public keys, unless MCSP has taken reasonable steps to verify that these 3rd party Secure Storage Subsystems comply with the requirements for Provisioned Secure Storage Subsystems.
- MCSP shall retain site security assurance on services and sites related to the provisioning of a Secure Storage Subsystem within Certified Products in at least one of the following three ways:

- Site Security assurance on services and related sites evaluated and certified by SOGIS (Senior Officials Group Information System Security) members consistent with ALC_DVS.2, or
- A Secure Storage Subsystem certification evaluated and Certified by SOGIS members to a protection profile at assurance level EAL4+ (EAL4 augmented by ALC_DVS.2) or higher, or
- ISO27001 certificate with a scope on all services and sites related to the provisioning and protection of the provisioned private/public keys. This ISO certificate shall be active and issued by a registrar accredited by an accreditation body that is a signatory of the International Accreditation Forum (IAF) Multilateral Recognition Arrangements (MLA).

1.5 Documentation and reporting

- MCSP shall have all key management related processes documented, such as key generation, certificate signing, certificate revocation, key archiving and back-up, and access management.
- MCSP shall provide traceability of issued Product Unit Certificates and Provisioned Secure Storage Subsystems by a revocation sequential identifier number in the certificates, upon request by WPC, provided that MCSP need not provide traceability for Product Unit Certificates and Provisioned Secure Storage Subsystems that were issued more than three (3) years before such request by the WPC. For the purpose of this clause, "traceability" means information about
  - the date when the certificate was created; and
  - when and to which party the Provisioned Secure Storage Subsystem was provided.
- MCSP need not provide information about events relating to Provisioned Secure Storage Subsystems that are not under its control. MCSP is not required to provide traceability of issued Product Unit Certificates and Provisioned Secure Storage Subsystems that are embedded into a Certified Product prior to leaving control of the MCSP.
- MCSP shall inform WPC, promptly after being notified, of any Provisioned Secure Storage Subsystem or private key related to the WPC, and under control of the MCSP, that was stolen, provided to an unauthorized 3rd party, or otherwise compromised. The previous sentence does not create an obligation to detect theft products in the supply chain of Provisioned Secure Storage Subsystems (that obligation can be elsewhere in this agreement).
- If MCSP believes that WPC's authentication system has been materially compromised, MCSP shall inform WPC. MCSP shall not be responsible for the accuracy or completeness of such information, and such information shall be deemed to be provided "AS IS" by MCSP to WPC. WPC shall not disclose the source of such information without MCSP's advance written authorization, nor take any action in direct response to the information. At WPC's discretion, WPC may conduct its own investigation of the potential compromising of its authentication system and act based on the results of its investigation. In regard to the foregoing, MCSP shall not be obligated to conduct any investigation nor to breach any contractual obligation.

2 Requirements for Manufacturer

2.1 General

- A Manufacturer may obtain signed Product Unit Certificates from one or more MCSPs.

2.2 Product Unit Certificates

- Manufacturer shall not use a Product Unit Certificate in a product with a WPC ID that is different from the WPCID of the Product Unit Certificate, except as specified in the next paragraph.
- Manufacturer may use a Product Unit Certificate only in a product in which the private key associated with that Product Unit Certificate is protected against compromise in a way that meets the requirements for Provisioned Secure Storage Subsystems (section 3 of this annex).

2.3 Secure Storage Subsystems

- Manufacturer shall not sell (or permit the sale of) any Manufacturer product that includes a Provisioned Secure Storage Subsystem to end users unless the product is a Certified Product or an authorized Test Platform.
- Manufacturer shall not provide a Provisioned Secure Storage Subsystem that is not embedded in the final product to any other party unless these Provisioned Secure Storage Subsystems remain under control of Manufacturer and Manufacturer keeps track of the location of these Provisioned Secure Storage Subsystems.

2.4 Documentation and reporting

- Manufacturer shall provide traceability of Provisioned Secure Storage Subsystems by a revocation sequential identifier number in the associated Product Unit Certificates, upon request by WPC, provided that Manufacturer need not provide traceability for Provisioned Secure Storage Subsystems that were issued more than three (3) years before such request by the WPC. For the purpose of this clause, “traceability” means information about:
  - the date each Provisioned Secure Storage Subsystem was provisioned or delivered to Manufacturer and;
  - the date each Provisioned Secure Storage Subsystem was embedded in the end product.
- Manufacturer need not provide information about events relating to Provisioned Secure Storage Subsystems that are not under its control. Manufacturer is not required to provide traceability of Provisioned Secure Storage Subsystems that are embedded into a Certified Product prior to leaving the Manufacturer’s control.
- Manufacturer shall inform WPC, promptly after being notified, of any Provisioned Secure Storage Subsystem or private key related to the WPC, and under control of the Manufacturer, that was stolen, provided to an unauthorized 3rd party, or otherwise compromised.
- If Manufacturer believes that WPC’s authentication system has been materially compromised, Manufacturer shall inform WPC. Manufacturer shall not be responsible for

the accuracy or completeness of such information, and such information shall be deemed to be provided “AS IS” by Manufacturer to WPC. WPC shall not disclose the source of such information without Manufacturer’s advance written authorization, nor take any action in direct response to the information. At WPC's discretion, WPC may conduct its own investigation of the potential compromising of its authentication system and act based on the results of its investigation. In regard to the foregoing, Manufacturer shall not be obligated to conduct any investigation nor to breach any contractual obligation.

3 Requirements for Provisioned Secure Storage Subsystems

A Provisioned Secure Storage Subsystem protects the private key that is associated with the public key in a Product Unit Certificate. Extraction of the private key makes it possible to use the signed Product Unit Certificate in products that are not Certified Products and that may create a safety risk for users of non-certified products.

At the time of manufacturing of the product, Provisioned Secure Storage Subsystems must be certified, and the certificate (or its renewal) shall be valid, with one of the following methods whose Security Target shall claim ECDSA with the curve NIST P-256 (or alternative names secp256r1, or prime256v1) for signature generation:

1. Provisioned Secure Storage Subsystems shall have a JIL Rating of High ("TOE resistant to attackers with attack potential of High") as defined in "Application of Attack Potential to Smart Cards" version 3.1 or later which requires review of the design, test and attack resistance of the SSS TOE. A lab accredited by a SOGIS member in the domain of smart cards and similar devices must perform the white box vulnerability assessment according to the aforementioned JIL standard. A summary report written by the accredited lab must be available to the WPC and Authorized Manufacturers to indicate that a JIL Rating of High has been achieved.
2. Provisioned Secure Storage Subsystems shall be built on hardware which carries a valid certificate according to one of the following:

   a) For Qi Certified Products:

   - Common Criteria Protection Profile EAL4+ PP0084
   - Common Criteria Protection Profile EAL4+ PP0035
   - Common Criteria Protection Profile EAL4+ PP0109
   - Common Criteria Protection Profile EAL4+ Automotive-Thin TPM ANSSI-CC-PP-2019/02 or later
   - Common Criteria Protection Profiles EAL4+ PP TPM-ANSSI-CC-PP-2018/03 or ANSSI-CC-PP-2020/01 or later
   - Common Criteria collaborative Protection Profile Dedicated Security Components cPP DSC v.1.0 & SD (Supporting Document) v1.0
   - GlobalPlatform `SESIP Profile for WPC Qi Secure Storage Subsystem' reference GPT_SPE_153

b) For Ki Certified Products

- Common Criteria Protection Profile EAL4+ PP0084
- Common Criteria Protection Profile EAL4+ PP0035
- Common Criteria Protection Profile EAL4+ PP0109
- Common Criteria Protection Profile EAL4+ Automotive-Thin TPM ANSSI-CC-PP-2019/02 or later
- Common Criteria Protection Profiles EAL4+ PP TPM-ANSSI-CC-PP-2018/03 or ANSSI-CC-PP-2020/01 or later

ANNEX B:
Revocation Rules and Procedure

1 Criteria for revoking certificates

Serial number in this text means “certificate serial number”.

1.1 Product Unit Certificates

1.1.1. Revocation by certificate serial number, or by revocation sequential identifier (“RSID")

A Product Unit Certificate may be revoked:

1. When the private key material related to that Product Unit Certificate has been compromised.
2. When a batch of Provisioned Secure Storage Subsystems is reported missing or stolen during transport.
3. When a certificate with that serial number is used to authenticate a product that is not a Certified Product.
4. When a certificate with that serial number is used to authenticate a product with a WPC ID that doesn’t match with the WPC ID in the certificate.

The WPC ID in the certificate matches with the product when

(a) The WPC ID of the product is the same as the WPC ID of the certificate.

(b) The product has been approved by WPC as a “Substantially Similar Product” variant of a Certified Product and the WPC ID of the original Certified Product is the same as the WPC ID of the certificate.

(c) The product is Certified as “contains a WPC certified subsystem” and the WPC ID of the subsystem is the same as the WPC ID of the certificate.

(d) The Manufacturer of the product has reported, before the product entered the market, that a limited number of these products contain a product unit certificate with this different WPC ID.

1.1.2. Revocation by WPC ID

All Product Unit Certificates that contain a specific WPC ID may be revoked:

1. When more than 20 Product Unit Certificates with this WPC ID have been revoked under rule 1.1.1.1.
2. When a Product Type was subject to a Final Non-Compliance Notice and is no longer a Certified Product, as the result of market inspection procedure in which a market sample of this product was found to be non-compliant.
3. When a Product Unit Certificate with this WPC ID is found in a product, purchased in

the market, that was subject to a Final Non-Compliance Notice.

4. When the product with this WPC ID is subject to a recall by a competent authority anywhere in the world. That includes without limitation, recall by the brand owner, importer, manufacturer, and consumer safety authorities.

1.2 Manufacturer CA Certificates

WPC may invalidate all Product Unit Certificates that were signed by a specific Manufacturer CA Certificate by revoking that Manufacturer CA Certificate:

1. When the private key of a Manufacturer CA Certificate is used by an unauthorized party to sign product unit certificates.
2. When more than 20 WPC IDs were revoked in certificates, signed by this Manufacturer CA Certificate under rule 1.1.2.1.

2 Certificate Revocation Procedure

Procedure for giving notice, and appeal when Manufacturer doesn't agree with the revocation decision of WPC.

2.1 Step 1:

WPC is informed of a possible need to revoke a certificate. That information may be provided by any party.

2.2 Step 2:

WPC reviews the evidence to verify that the criteria are met and evidence is documented.

2.3 Step 3:

WPC informs the owner of the certificate about the intention to revoke.

2.4 Step 4:

The owner of the certificate has 14 days to object.

The period to respond is reduced to 7 days when the revocation is under rule 1.1.2.4 (product recall).

2.5 Step 5a [no objection]

WPC implements the revocation. End of procedure.

2.6 Step 5b [objection]

A WPC expert group (consisting of volunteers from members without a relation to certificate owner) reviews the evidence and decides if the decision by WPC was correct or not.

2.7 Step 6a [decision by WPC was correct]

The owner of the certificate has 7 days to appeal.

Appeal is not possible when the certificate was revoked under rule 1.1.2.4 (product recall)

2.8 Step 6b [decision by WPC was not correct]

The certificate is not revoked. End of procedure.

2.9 Step 7 [appeal]

The owner of the certificate must pay the WPC an arbitration fee of $20,000 within 14 days which will be returned if appeal is successful.

2.10 Step 8:

Upon delivery of the arbitration fee, WPC will initiate arbitration by filing a Request for Arbitration with the ICC International Court of Arbitration. The parties agree, pursuant to Article 30(2)(b) of the Rules of Arbitration of the International Chamber of Commerce, that the Expedited Procedure Rules shall apply to the arbitration. The law of the arbitration will be the laws of the United States and the State of New York. The proceedings will be conducted in English. The proceedings will be conducted virtually to the maximum degree possible; if in-person meetings are required, they will be held in New York City, NY, USA. The scope of the arbitration will be limited solely and exclusively to the question of whether WPC made a correct revocation decision in accordance with the provisions of this Annex B. The sole and exclusive remedy available to the appealing party will be an order that WPC not execute on its revocation decision. Arbitration costs in excess of the arbitration fee will be shared equally, and each party will otherwise bear its own legal fees and expenses.

2.11 Step 9a [decision by WPC was correct]

WPC implements the revocation. End of procedure.

2.12 Step 9b [decision by WPC was not correct]

WPC refunds the arbitration fee. The certificate is not revoked. End of procedure.

ANNEX C:
Audit

WPC may audit Manufacturer CA Service Provider or Authorized Manufacturer (the "Auditee") premises up to one time in any twelve-month period ("Audit") at WPC's expense. Such audit shall be performed by an auditor ("Auditor") who is either an employee or agent of WPC or an independent third party agreed by the WPC and Auditee and shall occur during regular business hours at a time agreed by the parties. Before the Audit occurs, the Auditor shall sign an NDA with Auditee, and all information obtained during the Audit shall be deemed to be Auditee confidential information, provided that (a) an independent third party Auditor will be permitted to disclose all relevant information to WPC, and (b) WPC will be free to use such information as reasonably necessary to enforce its rights under this Agreement, provided that WPC must take reasonable steps to protect confidential or proprietary information of Auditee from public disclosure.

The scope of the Audit shall be limited to the materials reasonably needed to establish Auditee's compliance with its obligations under Annex A.

In the event that Auditor finds that Auditee has not materially complied with its obligations under Annex A, WPC and Auditee shall discuss such finding in good faith with the intention to ensure that WPC and Auditee share a common understanding of the security requirements of Annex A and to agree on changes (if any) to improve compliance with such requirements.

In the event that Auditor finds information that either (a) the parties mutually agree in good faith is a Material Breach (even if subsequently cured), or (b) is determined by a court or similar adjudicator to be a Material Breach, then Auditee will pay to WPC the reasonable costs incurred by WPC in connection with the Audit.

ANNEX D: Fees

Fees for a Manufacturer

Description	Amount	Due date
Manufacturer Annual Fee	US$ 0.-	N/A
Manufacturer CA Certificate Fee	US$ 0.-	N/A
Product Unit Certificate Fee	US$ 0.-	N/A

Payment terms

Payment terms are defined in the WPC's Financial Administration Policy.