verizon

IoT SECURITY CREDENTIALING SERVICES +

1. GENERAL

1.1 **Service Definition.** Verizon IoT Security Credentialing Services is a GSMA authorized service for Verizon to operate remote SIM provisioning services and/or provide eUICC to GSMA-approved third parties. The Services enables Customers to request and receive digital credentials from Certificate Authorities (CAs) created or hosted by Verizon, subject to availability. CAs and associated components for issuing Digital Certificates are based on a modified use of public key cryptography that is used for strong authentication, authorization, and privacy.

1.2 **License to Licensed Marks.** IoT Security Credentialing Services grants Customer an unlimited, non-exclusive, non-transferrable, royalty-free and sub-licensable right and license to use the Licensed Marks solely to indicate that Customer's Digital Certificates, keys, and signatures are GSMA Certified, as long as Customer remains compliant with GSMA requirement.

1.2.1 **Exclusion.** Customer is not permitted to disclose, copy, reproduce, modify or make available to third parties the Licensed Marks.

1.2.2 **Certificate Chaining.** Through digital signing, and by using the Verizon Root, Verizon will chain the Customer CA to the Verizon Root.

1.2.3 **Certificate Issuance.** Customer may only use Digital Certificates of the type and categories purchased in the Order.

1.2.4 **Termination of License to Licensed Marks.** Verizon may terminate Customer's license to use License Marks if Customer fails to comply with GSMA requirements and has not cured such failure within five Business Days of Verizon's written notice of such non-compliance. Upon termination, (a) the rights and licenses granted hereunder to Customer will immediately terminate; (b) Customer will be disassociated and/or removed from Verizon Roots; (c) each Party will promptly return to the other all proprietary and/or confidential material in its possession or under its control and received from the other Party under the Agreement, including all copies thereof.

~~1.2.1~~ **Continuation of Certain Provisions.** Termination or expiration of a Digital Certificate will not affect the continuance or force of any provision which is expressly, or by implication, intended to continue in force, on or after such termination or expiration. Upon termination of any Digital Certificate, Verizon will continue to maintain security certificates that were previously designated as GSMA Certified until such certificates

verizon

1.2.5 expire, unless such certification would otherwise violate the GSMA requirements (e.g., the certificates have been compromised).

2. **SUPPLEMENTAL TERMS**

2.1 **Customer Responsibilities**

2.1.1 **GSMA Requirements.** Customer will comply with all GSMA requirements, and will remain in compliance at all times. Customer acknowledges that GSMA may update its requirements from time to time upon at least 30 days' written notice and Customer will comply with such updated requirements when they are effective. GSMA requirements include, but are not limited to the below provisions.

2.1.1.1 **GSMA Approval.** Customer must obtain GSMA approval and be named a GSMA accredited party on the GSMA Portal (available at ~~http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme/sas-accredited-sites-list)~~www.gsma.com/solutions-and-impact/industry-services/assurance-services/security-accreditation-scheme-sas/sas-accredited-sites/) and remain in compliance with GSMA requirements.

2.1.1.2 **License Mark Brand.** Customer will use the Licensed Marks in accordance with GSMA's branding guidelines. Customer acknowledges that the GSMA branding guidelines may change at any time at GSMA's discretion.

~~2.1.1.1~~2.1.1.3 **Specifications.** Customer is subject to the following requirements:

- ~~●~~SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification ~~v3.1~~v4.2 dated ~~May 27, 2016~~July 7, 2020 ("SGP.02") (~~http://www.gsma.com/newsroom/all-documents/sgp-02-v3-1-remote-provisioning-architecture-for-embedded-uicc-technical-specification/~~www.gsma.com/solutions-and-impact/technologies/esim/gsma_resources/sgp-02-v4-2/);
- SGP.14 GSMA eUICC PKI Certificate Policy ~~v1.0~~v2.1 as the terms existed on ~~November 1, 2016;~~February 11, 2021 (www.gsma.com/solutions-and-impact/technologies/esim/gsma_resources/gsma-euicc-pki-certificate-policy-v21/); and
- SGP.22 RSP Technical Specification Version ~~1.1~~2.4 dated ~~June 9, 2016 (http://www.gsma.com/newsroom/all-documents/sgp-22-technical-specification-v1-1/~~October 28, 2021 (www.gsma.com/solutions-and-impact/technologies/esim/gsma_resources/sgp-22-technical-specification-v2-4/).

~~2.1.1.3~~2.1.1.4 **Use of Names.** Customer will manage, supervise, and audit, their operators or owners use of names in their certificate applications that Customer knows or has reason to believe are protected intellectual property.

~~2.1.1.4~~2.1.1.5 **Non-Compliance.** In the event that Customer is no longer in compliance with GSMA requirements, Customer will immediately notify Verizon as soon as Customer knows of its deviation from the GSMA requirements. If Customer fails to comply with this Section 2.1.1.5 and/or any GSMA requirements in Section 2.1.1.2 and 2.1.1.3, Verizon will remove or disassociate Customer from the Verizon Root or otherwise suspend it if Customer fails to take corrective or remedial action within five Business Days of Customer's non-compliance.

~~2.1.1.5~~2.1.1.6 **Customer CA Operators.** Customer is responsible for ensuring that only suitably skilled and qualified administrators are appointed and authorized to operate the Customer CA. Customer will operate the Customer CA in compliance with the then current industry standards, including the

applicable standards regarding personnel security and the physical, administrative, and logical security of a certification authority infrastructure, including storage of each Customer CA on a secured hardware signing module.

~~2.1.1.6~~ **Customer Environment.** Customer acknowledges and accepts that changes to the Customer's ecosystem or network environment and/or configuration (such as, inter alia, changes in the software and/or hardware deployed by Customer to operate the **Customer** CA) may affect the Customer CA.

2.1.1.7 Verizon will not be responsible for any costs, expenses or liabilities incurred by Customer in connection with Customer's operation of the Customer CA.

2.1.1.8 **Third Party Signature/Cross-Signature.** Customer will not allow any third party signature or cross-signature of the Customer CA or obtain services similar to these Services from any third party during the term of the Contract.

2.1.1.9 **Customer Equipment.** Customer acknowledges and accepts that it will be solely responsible for the incorporation of any hardware components or computer code containing the Customer CA into other machines, components, applications, logic, computer code, endpoints, ecosystem, network, or any combinations thereof.

2.2 ~~2.2~~ **Intellectual Property (IP) Rights.** IP Rights in and to Proprietary Materials are owned and will continue to be exclusively owned by Verizon and/or its licensors. Customer agrees to make no claim of interest in or to any such IP Rights. Customer acknowledges that no title to the IP Rights in and to the Proprietary Materials is transferred to Customer and that Customer does not obtain any rights, express or implied, in any Proprietary Materials other than the rights expressly granted in the Agreement herein. Customer will not, and will not enable others to, for any purpose not expressly permitted under the Agreement, copy (except for backup purposes), modify, redistribute, reverse engineer, decompile, create derivative works, disassemble or otherwise attempt to derive the source code, techniques, processes, algorithms, know-how or other information from the Services rendered hereunder.

2.3 **Records and Reporting.** Customer will keep reasonable records relating to any of Customer's responsibilities and obligations under a Contract. Within 30 calendar days following each Order Anniversary Date, Customer agrees to certify to Verizon in writing: (i) the total number of certificates issued under or from the Customer CA; and (ii) its compliance with the terms and conditions of this Service.

2.4 **Audit.** During the term of the Contract and for a period of one calendar year thereafter, Verizon may, upon reasonable notice and during Normal Business Hours, periodically audit Customer's compliance with terms of this IoT Security Credentialing Service. In the event any such audit discloses any material breach by Customer (or its employees or agents) of its obligations hereunder, Customer will, in addition to such other rights and remedies that may be available to Verizon, refund Verizon the reasonable costs and expenses incurred by Verizon in connection with such audit.

2.5 **Export Controls.** Customer will not solicit and will not accept any certificate applications from any person or organization that is on the most recent United States export exclusion lists, and will not engage in any transaction (in whole or in part) in any country subject to any United Nations, USA, Australia or European Union embargo, regulation, terrorist controls or other similar restriction. Customer represents and warrants that any authorized user is not located in, under the control of, or a national or resident of any such country or on any such list.

3. FINANCIAL TERMS

3.1 **General.** Customer will pay the applicable fee for the Service as shown in the Contract.

verizon

4. **DEFINITIONS**

Term	Definition
Authorized Certificate Issuer	The Customer
Certificate Authority	An entity that issues Digital Certificates, acting as a third party which is trusted both by the owner of the Digital Certificate and by the party relying upon the Digital Certificate.
Customer CA	Customer's Digital Certificates chained to the Verizon Root.
Digital Certificate	The cryptographic binding that can be used to enhance digital privacy, authenticate a trusted identity and then to authorize that identity to access protected resources, (e.g. sub certificate authorities, web service, data, applications, VPNs, Wi-Fi networks, and infrastructure communications such as server communications and machine-to- machine applications).
eUICC	Embedded Universal Integrated Circuit Card
GSMA	GSMA Limited, the trade body that represents the interests of mobile network operators worldwide.
GSMA Certified	Customer's Digital Certificates, keys, and signatures are compliant with GSMA License Mark and Specification requirements set forth herein.
IoT	Internet of Things
IP Rights	All title, copyrights, trademarks, service marks, patents, patent applications and all other intellectual proprietary rights now known or hereafter recognized in any jurisdiction.
Licensed Marks	The following word marks: GSMA; GSMA Certified.
Proprietary Materials	Verizon's technology, web sites, documentation, products and services.
SIM	Subscriber Identification Module
Verizon Root	~~Digital signing, and by using private keys cryptographically related to a~~ A private root key that is chained to a digital certificate root that is owned and operated by Verizon.