



ENTRUST

NCIPHER SECURITY IS AN ENTRUST COMPANY

nShield as a Service (“nSaaS”) Offering Schedule

Service Overview

The nSaaS Offering provides a secure, hosted solution for storing, managing, and using cryptographic keys via hardware security modules (HSMs). The nSaaS hosted model is designed to be straightforward and simplifies the implementation of cryptographic services by limiting Customer’s involvement with HSM management to client software and credentials. All other elements of the Offering will be controlled and managed by Entrust for the Customer.

Capitalized terms not defined in this Schedule have the meanings given to them in the [General Terms](#) or other Schedules applicable to the nSaaS Offering.

1. Service Details

Subject to the Agreement, Entrust will provide the following as part of the nSaaS Offering:

- a. One of Entrust’s technical experts to serve as the overall primary contact for Customer in order to ensure a successful nSaaS experience.
- b. Access to and use of one (1) or more dedicated HSM(s), hosted on a FIPS 140-2 level 3 HSM(s)
- c. Any smart card reader and a set of smart cards as required by the HSM(s).
- d. Implementation and configuration of the HSM(s).
- e. For fully managed HSM(s) offering only: Professional operational management of the HSM(s) under high assurance security policies and procedures including:
 - i. Dual Control for HSM(s) administration
 - ii. Role separation with assigned roles for HSM administrators and Customer cryptographic users.
- f. Secure handling and storage of all HSM(s) components , smartcards and passphrases according to Entrust and nSaaS policies and procedures.

2. Offering Specific Indemnity:

Customer will indemnify, defend and hold harmless Entrust and its Affiliates from and against any and all claims, arising out of or related to: (i) Customer’s alleged or actual misuse of the nSaaS Offering. Misuse shall comprise any use of the nSaaS Offering in an unauthorized manner including without limitation in breach of acceptable use policy attached as Appendix A to this Schedule (“AUP”) (ii) Claims related to infringement, misappropriation or violation of a copyright, trademark, trade secret, or privacy or confidentiality right by written material, images, logos or other content uploaded to the nSaaS Offering.

3. Assumptions and Limitations:

The nSaaS Offering is subject to the following assumptions and limitations:

- a) The nSaaS Offering will implement and operate only using the HSMs owned and managed by Entrust in authorized Entrust selected data center facilities;
- b) Networking-based assumptions and limitations:
 - i. Customer will provide its own means of network connectivity via dedicated network connection or Internet Service Provider for access to the data center and service environment.
 - ii. Customer will have facilities to terminate VPN tunnels as specified by Entrust.
 - iii. Customer will perform support, troubleshooting or monitoring of its communications infrastructure and components, network (LAN or WAN) for the purposes of problem resolution.



ENTRUST

NCIPHER SECURITY IS AN ENTRUST COMPANY

iv. Network accessibility from Customer sites to external networks or the Internet is outside the scope of nSaaS.

4. Customer Roles and Responsibilities

Customer will be responsible for the following:

- a. Identifying a primary technical point of contact within Customer's organization with respect to the Offering.
- b. Providing assistance in identifying representatives from Customer's various internal and external stakeholders who have an interest or are affected by the Offering.
- c. Facilitating scheduling of stakeholder representatives to participate in the exchange of information with Entrust.
- d. Responding in a timely fashion to questions posed by Entrust regarding the Offering.
- e. In self-managed installations, initializing the HSM(s) with the applicable Software and maintaining control over the applicable administrator card set
- f. Maintaining backups of the Customer data, including key files, stored on the customer's client host(s)

5. Policy and Compliance

The nSaaS Offering will be operated in ISO 27001 compliant facilities according to the operational standards laid down in Entrust's corporate security policies.

6. Term

Unless a different duration is set out in the Order, the nSaaS Offering is provided on a 3-year subscription term ("Term"). The Term can be extended by renewal as set out in the General Terms. All subscriptions are non-cancellable and non-refundable.

In addition to the Parties' termination rights as covered within the General terms, Entrust can at its sole discretion, suspend Customer's access to the nSaaS Offering, upon reasonable notice, for the following reasons: (i) violation of the AUP or other breach of the Agreement, in each case to a material degree; (ii) subjecting Entrust to potential material liability or interfering with the use of the nSaaS Offering by other Entrust customers; (iii) Entrust deems it reasonably necessary to do so to respond to any actual or potential security concerns; (iv) violation of applicable laws, rules or regulations; (v) for scheduled or emergency maintenance. If any such use described in (i) to (iv) of this Section 6 is not remedied within a reasonable period of time following such suspension then Entrust may, at its sole discretion, terminate Customer's access to the nSaaS Offering (whole or in part) upon reasonable advanced written notice to Customer. For the avoidance of doubt, Entrust shall not suspend or terminate Customer's use of or access to the nSaaS Offering where it can suspend or terminate access for an individual user which is in default under this Section 6.

Entrust may either suspend provision of nSaaS Offering (whole or in part) or terminate the Agreement, in each case, where reasonably possible, by giving not less than ninety (90) days' prior written notice to Customer, where Entrust must end the Agreement or nSaaS Offering due to a legal or regulatory reason or third party service provider and/or licence requirements. In the event that Entrust exercises its right to terminate the Agreement or an Offering (whole or in part) under this paragraph, Entrust shall refund on a pro-rated basis any prepaid fees for the remaining nSaaS Offering subscription that remains unused due to such termination.

7. Service Levels and Support

Entrust provides the service level and support commitments for the nSaaS Offering as set out in the [nSaaS Support Schedule](#).



ENTRUST

NCIPHER SECURITY IS AN ENTRUST COMPANY

Appendix A

ACCEPTABLE USE POLICY

This Acceptable Use Policy (“**AUP**”) describes actions that Entrust prohibits when any party uses the nSaaS Offering (the “**Service**”). The examples described in this AUP are not exhaustive. References to “Entrust” shall also include, in addition to the Entrust contracting entity, its affiliates, subsidiaries, licensors, and other service providers. The Agreement contains definitions of capitalized terms not otherwise defined in this AUP and such definitions shall apply in this AUP (unless otherwise specified). The Agreement takes precedence over any conflicting provisions in this AUP. Entrust may modify this AUP at any time. Entrust will take commercially reasonable efforts to provide You with written notice (email or posting notice at the Service portal to suffice as adequate notice). By using the Service, You agree to the latest version of this AUP. If You violate the AUP or authorize, encourage or help others to do so, we may suspend or terminate Your use of the Service.

Thus, You agree not to use, and not to encourage or allow any end user to use, the Service in the following prohibited ways.

No Illegal, Harmful, or Offensive Use or Content

You may not use, or encourage, promote, facilitate or instruct others (i) to use the Service for any illegal, harmful, fraudulent, infringing, abusive or offensive use, or for any other activities that materially interfere with the business or activities of Entrust; or (ii) to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, fraudulent, infringing or offensive. Prohibited activities or content include, without limitation:

- **Illegal, Harmful or Fraudulent Activities.** Any activities that: (i) are illegal, that violate the rights of others, or that may be harmful to others, Entrust operations or reputation, including disseminating, promoting or facilitating child pornography, offering or disseminating fraudulent goods, services, schemes, or promotions, make-money-fast schemes, ponzi and pyramid schemes, phishing, or pharming; (ii) violate or facilitate the violation of any local, state, provincial, federal, or foreign law or regulation, including, but not limited to, laws and regulations regarding the transmission of data or software and recording of phone calls and communications; (iii) use the Service in any manner that materially violates telecommunications industry standards, policies and applicable guidelines published by generally recognized industry associations, including those specifically communicated in writing to You by Entrust; (iv) use the Service to harvest or otherwise collect information about individuals, including email addresses or phone numbers, without their explicit consent or under false pretenses; (v) violate the privacy or data protection rights of any person (e.g. collecting or disclosing any information about an identified or identifiable individual protected under the privacy and/or data protection legislation applicable in the individual’s jurisdiction without written permission); constitute cooperation in or facilitation of identity theft; (vi) degrade or negatively influence the good will or reputation of Entrust or that of its affiliates, customers, partners or other third party service providers; or (vii) use the Service in a manner that triggers a law enforcement, government, or regulatory agency to request the suspension of the Service to Customer and/or its related phone numbers.
- **Infringing Content.** Content that infringes or misappropriates the intellectual property or proprietary rights of others.
- **Offensive Content.** Content that: (i) is defamatory, illegal, obscene, offensive, inappropriate, pornographic, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts; or (ii) is, facilitates, or encourages libelous, defamatory, discriminatory, or otherwise malicious or harmful speech or acts to any person or entity, including but not limited to hate speech, and any other material that Entrust reasonably believes degrades, intimidates, incites violence against, or encourages prejudicial action against anyone based on age, gender, race, ethnicity, national origin, religion, sexual orientation, disability, geographic location or other protected category;
- **Harmful Content.** Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, spyware, worms, time



ENTRUST

NCIPHER SECURITY IS AN ENTRUST COMPANY

bombs, cancelbots, or any other malicious, harmful, or deleterious programs.

No Security Violations

You may not use the Service to violate the security or integrity of any network, computer or communications system, software application, or network or computing device, including, without limitation, the computers used to provide the Service (each, a “**System**”). Prohibited activities include:

- **Unauthorized Access.** Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.
- **Interception.** Monitoring of data or traffic on a System without permission.
- **Falsification of Origin.** Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route (including creating a false phone number), or otherwise attempting to mislead others as to the origin of a message or phone call. The legitimate use of aliases and anonymous remailers is not prohibited by this provision.
- **Creating False Identity.** Creating a false identity or phone number, or otherwise attempting to mislead others as to the identity of the sender.

No Network Abuse

You may not make network connections to any users, hosts, or networks unless You have permission to communicate with them. Prohibited activities include:

- **Monitoring or Crawling.** Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled.
- **Denial of Service (DoS).** Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective. Launching or facilitating, whether intentionally or unintentionally, a denial of service attack on the Service or any other conduct that materially and adversely impacts the availability, reliability, or stability of the Service.
- **Computer Viruses.** Do not intentionally distribute a computer virus or in any other way attempt to interfere with the functioning of any computer, communications system, or website, including the computer, and communications systems used to provide the Service. Do not attempt to access or otherwise interfere with the accounts of customers and/or users of the Service or the Service itself;
- **Intentional Interference.** Interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques.
- **Operation of Certain Network Services.** Operating network services like open proxies, open mail relays, or open recursive domain name servers.
- **Avoiding System Restrictions or Security Mechanisms.** Using manual or electronic means to avoid, bypass or break any use limitations placed on a System, such as access and storage restrictions, or otherwise attempting to penetrate or disable any security system or mechanisms. Using the Service in any other manner that poses a material security or service risk to Entrust or any of its other customers. Reverse-engineering the Service in order to find limitations, vulnerabilities, or evade filtering capabilities.



ENTRUST

NCIPHER SECURITY IS AN ENTRUST COMPANY

No E-Mail or Other Message Abuse

You will not distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like “spam”), including commercial advertising and informational announcements. You will not alter or obscure mail headers or assume a sender’s identity without the sender’s explicit permission. You will not collect replies to messages sent from another internet service provider if those messages violate this AUP or the acceptable use policy of that provider.

Engaging in any unsolicited advertising, marketing or other activities prohibited by applicable law or regulation covering anti-spam, data protection, or privacy legislation in any applicable jurisdiction, including, but not limited to anti-spam laws and regulations such as the CAN SPAM Act of 2003, the Telephone Consumer Protection Act, and the Do-Not-Call Implementation Act.

Using the Service in connection with unsolicited, unwanted, or harassing communications (commercial or otherwise), including, but not limited to, phone calls, SMS or MMS messages, chat, voice mail, video, or faxes.

Our Monitoring and Enforcement

We reserve the right, but do not assume the obligation, to investigate any violation of this AUP or misuse of the Service. We may:

- investigate violations of this AUP or misuse of the Service; or
- remove, disable access to, or modify any content or resource that violates this AUP or any other agreement we have with You for use of the Service.

We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP.

Reporting of Violations of this AUP

If You become aware of any violation of this AUP, You will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation.