NSHIELD AS A SERVICE WEB

PRIVACY NOTICE

Contents

nShield as a Service (nSaaS) Web

Last updated: December 4, 2023

nSaaS Web

This product privacy notice describes how nSaaS Web collects and processes personal data pursuant to applicable data privacy laws.

Description

nShield as a Service Web provides high assurance cryptography as a service using RESTful APIs, providing developers with a modern mechanism to build applications requiring access to cryptographic resources underpinned by an nShield HSM resilient root of trust.

Personal Data Collection and Processing

Customers control the types of data to be encrypted or decrypted using the service. The Entrust nSaaS Web service receives a request from a Customer application to perform a cryptographic operation, the data is received by a Web Server operating in a private VPC environment dedicated to the customer before being passed to one of the Entrust-hosted HSMs allocated to the Customer, the cryptographic operation is performed, and the data is returned, via the Web Server, to the Customer.

Entrust collects the Customer's public IP address associated with the outbound connection to the AWS hosted web service and maintains an "allow list" to prevent access from unauthorized IP addresses.

nSaaS Web also processes the source data stream, terminating the incoming TLS tunnel in the internal web-server, before opening a new TLS channel for onward transmission of the data stream to the hosted HSM. Thus, the certificate authenticating the customer's application to the service and the contents of the data stream are temporarily present in the server memory. None of this data is collected or retained.

Retention Period

Entrust does not retain any Customer data beyond the duration of the cryptographic operation being performed except for the Customer's public IP addresses, which are retained for the duration of the service.

Use of Sub-Processors

For the current list of sub-processors, visit https://www.entrust.com/legal-compliance/privacy/sub-processors.

International Data Transfers

nSaaS Web makes use of data centers in the United States. If a customer is located in a different country than the United States, and any data streams transmitted to the hosted HSMs include personal data, then there may be cross-border transfers of personal data. Any cross-border transfers of personal data are made in accordance with relevant data privacy law requirements (e.g., the Standard Contractual Clauses for EU personal data transferred out of the EU).

Data Protection Measures

For more information on how Entrust processes personal data collected by this product, please refer to Schedule 1 of our standard customer data processing addendum (DPA) found here.

Legal Basis for Processing Personal Data

The legal basis for the processing personal data by nSaaS Web is performance of a contract.

Artificial Intelligence (AI) and Automated Decision-making (ADM)

nSaaS Web does not make use of artificial intelligence or automated decision-making.

Data Privacy Rights

The Customer is the data controller for all personal data processed by nSaaS Web. Entrust Corporation, as the data processor, will assist the Customer, to the extent reasonable and practicable, in responding to verified data subject access requests the Customer receives with respect to nSaaS Web.

Amendments to this Privacy Notice

We reserve the right to amend this Product Privacy Notice from time to time as our business, laws, regulations and industry standards evolve. Any changes are effective immediately following the posting of such changes to https://www.entrust.com/legal-compliance/data-privacy/product-privacy-notices. We encourage you to review this notice from time to time to stay informed.

Contact Information

For questions about this product privacy notice, please contact privacy@entrust.com. For Entrust Corporation's general web privacy notice, please click here.