Additional License Authorizations

For OpenText™ Data Privacy and Protection software products

This Additional License Authorizations document ("ALA") sets forth the applicable License Options and additional specific software license terms that govern the authorized use of the software products specified below, and are part of the applicable agreement (i.e., Micro Focus End User License Agreement; and/or any separate agreement that grants Licensee a license to such products, e.g., Customer Portfolio Terms or other Master Agreement; and/or Quotation) (the "Applicable Agreement"). Capitalized terms used but not defined herein shall have the meanings set forth in the Applicable Agreement. All products below are delivered electronically, and as such, any reference to software delivery methods that are stated on the purchase order other than electronic are void.

Products and Product Suites

Products

Product Line	Product	Non-production software class[*]	Term License Non-production software class (if available)
Data Privacy and Protection APIs			
	Data Privacy and Protection File Processor (Voltage SecureData File Processor)	Class 3	Class 3
	Data Privacy and Protection Simple API (Voltage SecureData Simple API)	Class 3	Class 3
	Data Privacy and Protection z/Protect (Voltage SecureData z/Protect)	Class 3	Class 3
Data Privacy and Protection Foundation			
	Data Privacy and Protection Appliance (Voltage SecureData Appliance)	Class 2 & 3**	Class 3
	Data Privacy and Protection Services (Voltage SecureData Services)	Class 2 & 3**	Class 3
Data Privacy and Protection Integrations			
	Data Privacy and Protection for AWS (Voltage SecureData Integrations for AWS)	Class 3	Class 3
	Data Privacy and Protection for Azure (Voltage SecureData Integrations for Azure)	Class 3	Class 3
	Data Privacy and Protection for GCP (Voltage SecureData Integrations for GCP)	Class 3	Class 3
	Data Privacy and Protection for Hadoop (Voltage SecureData Integrations for Hadoop)	Class 3	Class 3
	Data Privacy and Protection for Snowflake (Voltage SecureData Integrations for Snowflake)	Class 3	Class 3
	Data Privacy and Protection for Teradata (Voltage SecureData Integrations for Teradata)	Class 3	Class 3
Data Privacy and Protection Interception			
	Data Privacy and Protection Sentry (Voltage SecureData Sentry)	Class 3	Class 3
Data Privacy and Protection Payments			
	Data Privacy and Protection Host SDK (Voltage SecureData Host SDK)	Class 2 & 3**	Class 3
	Data Privacy and Protection Mobile SDK (Voltage SecureData Mobile SDK)	Class 2 & 3**	Class 3
	Data Privacy and Protection Terminal SDK (Voltage SecureData Terminal SDK)	Class 2 & 3**	Class 3
	Data Privacy and Protection Web (Voltage SecureData Web)	Class 2 & 3**	Class 3

Product Line	Product	Non-production software class*	Term License Non-production software class (if available)
SecureMail			
	SecureFile (Voltage SecureFile)	Class 3	Class 3
	SecureMail (Voltage SecureMail)	Class 3	Class 3
SmartCipher			
	SmartCipher (Voltage SmartCipher)	Class 3	Class 3
Structured Data Manager			
	Structured Data Manager (Voltage Structured Data Manager)	Class 1	Class 3
	Database Activity Monitoring (Voltage Database Activity Monitoring)	Class 1	N/A

*Non-production use rights, if any, can be found at **opentext.com/about/legal/software-licensing**.

**Specific parts of this product offering have Non-Production licenses for Development and Test and for Disaster Recovery purposes, those are Class 2; all other parts of this product offering are Class 3.

Product suites

There are no current product suites.

Legacy Product Suites
The following product suites were used in previous license models. They are included here as customers may currently hold licenses for these suites but they are no longer available for sale.

Suite	Perpetual License Non-production use category*	Term License Non-production software class (if available)
SecureData Enterprise Data Warehouse Starter Edition	Class 3	Class 3
SecureData Enterprise Data Warehouse Enterprise Edition	Class 3	Class 3
SecureData Enterprise Infrastructure Suite 1 – Production and Test and Development	Class 2	Class 3
SecureData Enterprise Infrastructure Suite 1 – Disaster Recovery	Class 2	Class 3
SecureData Enterprise Infrastructure Suite 2 – Production and Test and Development	Class 2	Class 3
SecureData Enterprise Infrastructure Suite 2 – Disaster Recovery	Class 2	Class 3
SecureData Suite for Hadoop Starter Edition	Class 3	Class 3
SecureData Suite for Hadoop Enterprise Edition	Class 3	Class 3
SecureData Suite for Open Systems Standard Edition – Test and Development	Class 2	Class 3
SecureData Suite for Open Systems Enterprise Edition – Test and Development	Class 2	Class 3

*Non-production use rights, if any, can be found at **opentext.com/about/legal/software-licensing**.

Definitions

Capitalized terms not otherwise defined in this ALA document are defined in the governing agreement.

Term	Definition
Acquirer	When referring to a payment processor entity, an organization that facilitates electronic payment authorization and/or settlement for payment transactions and related services.
Application	A single module or service, or a collection of integrated software modules or services, or a distinct process designed to perform a specific single Organization Function. For SecureData, in particular, the Organization Function must include the transacting, processing, or storing of protected data. Any Application that uses SecureData or SecureMail indirectly, such as via a service, microservice or proxy, must be licensed as a separate Application.
Ciphertext	The result of protecting cleartext through encryption, hashing, or tokenization.
Cleartext	Data that has not been protected, whether human-readable or not; compare with "plaintext"
Cold Standby System	A secondary standby non-production system that is not handling any transactions or being otherwise used, and is also NOT up and running. If the primary production system breaks down, or needs to be taken out of service, the Cold Standby System will be started to take over for the primary production system.
Core	A discrete package of an arithmetic-logic unit, instruction unit, and registers that are autonomously able to address random access memory and execute a software program.
COTS	Commercial-Off-The-Shelf software.
Database	A container that stores application data including table structure, stored procedures, and other functionality that runs on a Database Instance.
Database Instance	A software application that has the sole purpose of acting as a container that hosts and executes one of more Databases.
Data Center	A single, physical collection of networked computer systems with a defined geographic location. For public cloud services providers, a Data Center is an Availability Zone. Availability Zones (AZ) are unique physical locations within Cloud Service Provider Region. Each AZ is made up of one or more datacenters equipped with independent power, cooling, and networking.
Developed Code	The software and scripts developed and/or deployed by licensee using Voltage products.
Development System	A non-production development system that has a software product installed and is to be used for developing software product add-on applications.
Device	An addressable entity, physical or virtual, including but not limited to router, switch, bridge, hub, server, PC, laptop, handheld device, or printer that resides within the range defined for interrogation and asset tracking.
Disaster Recovery (DR) System	A Cold-Standby System or Hot-Standby System.
Driver Interception	The interception of an application's database API calls (e.g., over JDBC or ODBC) by a Sentry driver wrapper.
Encryption	A key-based, cryptographic transformation of sensitive data into a non-sensitive de-identified form (ciphertext).
Endpoint	A device or system that a user interacts with.
External Application	An Application that a customer does not own but uses through a subscription or term license (e.g., a SaaS application, such as Salesforce).
External User	A person who is not a contractor or employee of the licensee.
Event	A single protection; access; field discovery and classification; test data record creation; data record archival; or record deletion operation.

Term	Definition
Format-Preserving Encryption	Means an encryption algorithm that produces output of the same size and format as the input. For example, if the input comprises all digits, the output will also consist of digits.
Format-Preserving Hash	A keyed hash algorithm that produces output of the same size and format as the input. For example, if the input comprises all digits, the output will also consist of digits.
Gateway	Means an intermediary organization or service that facilitates data exchange between merchants and processors and may provide additional value-added service offerings to facilitate merchant needs. Gateways can be independent organizations or associated directly with a processor.
Hot Standby System	A secondary non-production system that is not handling any transactions but is up and running, ready to take over from the production system if the primary production system breaks down or needs to be taken out of service.
IFL	Integrated Facility for Linux, a Processor dedicated to Linux workloads on IBM Z systems.
Implementation	An installation of the software on a single Server, or installed on a cluster of Servers which work together as a single installation of the software.
Installation Kit	A collection of software products in ready-to-install form.
Instance	Each implementation of the software installed on a either a Physical or a Virtual Server.
Internal Application	An Application that a customer owns, such as through self-development or from a perpetual use license. This may include COTS applications.
Internal User	A person who is a contractor or employee of the licensee who has Use rights.
Key Server	An appliance configured to provide key management and key derivation services per configurable policies.
Lane	In retail environment a single payment terminal, either an electronic card reader or virtual terminal but not both, is connected to a single point of sale (cash register) to collect cardholder data for electronic payments (typically credit/debit card payment data).
Masking	Obfuscating data using FPE or SST to protect sensitive data such as payment card numbers, national identification numbers, and so on. Masked data can be used within test, development, analytics, or production environments.
Merchant	A payment-accepting business. Merchants may engage in either or /both of card-present physical or/and card-not-present transactions (e-Commerce stores).
Mobile	Personal computing devices running some COTS operating system.
MSU (Millions of Service Units)	The IBM standard rating of computing work capacity.
Named Application	See Application.
Node	Any computing Server where a datastore application software is running and where SecureData APIs are deployed, and/or where data protected by SecureData is stored, processed or used.
Organization Function	An activity carried out by an organization that yields income for the organization (a core organization function) or supports an activity that yields income for the organization (a support organization function).
PAN	As defined by PCI Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS,) version 3.2: "Acronym for 'primary account number', also referred to as 'account number.' Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account."
PCI	Payment Card Industry, a global forum that brings together payments industry stakeholders to develop and drive adoption of data security standards and resources for safe payments worldwide.

Term	Definition
Petabytes (PB)	10^{15} bytes, designating an amount of physical data capacity.
Physical Server	A Server that runs with an operating system directly controlling hardware, sometimes called "bare metal." This definition excludes a Server that runs with a hypervisor directly controlling hardware instead.
Plaintext	Data/information that has not been protected using Encryption, Hashing, or Tokenization and is printable—that is, contains no control characters or other unprintables; human-readable characters. Compare with "cleartext".
Point of Encryption	A device deployed for the purpose of allowing a business entity to capture and apply encryption and or tokenization to sensitive data. Devices include but are not limited to purpose-built terminals; devices with integrated terminals; and Commercial Off the Shelf (COTS) devices. Such Devices support PAN, SAD, or other sensitive data capture through various means of data conveyance, including but not limited to manual entry, electromagnetic, radio (NFC,) visual, and audio.
POS	Point Of Sale. Includes purpose-built hardware and software combinations as well as COTS devices with POS application(s) installed, web-based POS solutions, and unattended devices such as kiosks, vending machines, and access control devices capable of conveying fees and taking payments. products/components/suites.
Processor	When referring to a payment processor entity, an organization that facilitates electronic payment authorization and/or settlement for payment transactions and related services.
Proxy Interception	For SecureData Sentry, the interception of Application data (e.g., over HTTP/S) by a Sentry ICAP server.
Record	A set of related data stored in a data set (file) or table. A record can contain one or more values. Groups of records are saved in a data set or database table, in a defined format.
SAD	Sensitive authentication data as defined by PCI Point-to-Point Encryption, version 3.0: "Security-related information (including, but not limited to, card validation codes/values, full-track data from the magnetic stripe, magnetic-stripe image on the chip or elsewhere, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions."
Sensor	A SmartCipher endpoint client software that is installed on a supported end user device.
Server	Any designated computer system in which an Instance or Instances of the software is installed.
Suite	Two or more software products combined into a single license offering or a single software product that includes two or more licenses. The specific software products included in a Suite are specified in the Software Specific License Terms below. Software products included in a Suite are governed by the individual authorizations and use restrictions associated with each software product except where specified in the specific Suite software specific license terms below.
Terabytes (TB)	10^{12} bytes, designating an amount of physical data capacity.
Term License to Use *or* Term LTU	A software license to use (LTU) that indicates in its license description that the license is valid for a specific period of time such as One Month (1M), One Year (1Y) etc. Term LTUs are not perpetual licenses.
Term Support	A fixed-period support offering that is only valid during the time period of the associated Term LTU.
Terminal	A purpose-built device with hardware and software capabilities to capture PAN and or SAD data.
Test System	A non-production test system that has a software product installed and is to be used for a) software product migration testing, and/or b) software product pre-production staging.
Tier	The level of Processors or Merchants as determined by annual card payment transaction volume. For Processors, the Tier level is based on the industry standards of tiering which are determined by the annual volume of payment transactions. For Merchants, the Tier level is based on the PCI Data Security Standard (DSS) tiering definitions, which are determined by the Merchant's annual payment card transaction volumes.
Token	A surrogate value created by a Tokenization process. A token shares some of the characteristics of the original data element, such as format, length, etc., and is deterministically created, i.e., repeatedly asking for a token for a given data item will yield the same token.

Term	Definition
Tokenization	A process by which sensitive data elements, such as PANs, Personal Identifiable Information, etc. are replaced by surrogate values. The surrogates can replace the cleartext value in databases, applications, and data stores. The process can be reversible or irreversible, and may be cryptographic or non-cryptographic. The term Tokenization is frequently used to mean any format-preserving data protection. Voltage SecureData offers various tokenization techniques such as FPE, eFPE, FPH, and SST.
Transaction	The transfer of data from a point of capture to a destination host. Transactions may involve payment card data, or capture and transfer of other values including credentials, tax IDs, and other regulated sensitive data. For payments data, the volume of transactions includes payment card authorization requests (including zero-dollar requests) to the host, in addition to authorization and settlement requests. The total transaction volume therefore includes standalone authorization requests, authorization and settlement requests, and card validation requests.
Unlimited events	That the number of events that can be consumed by a customer has no limit within the length of the subscription. Refer to Licensing Unlimited Events SKUs section under Software specific license terms for further details.
Use	To install, store, load, execute, and/or view one copy of the software and/or its function(s).
User	A user whose Use is restricted to the type of software that is being licensed.
User Pack	A predetermined number of Users.
Virtual Machine	A computer that does not physically exist but is simulated on another computer.
Virtual Server	A Virtual Machine running an operating system controlling hardware not directly but via a hypervisor. A computer running a hypervisor may run more than one Virtual Machine at the same time.
Virtual Terminal	A web-based solution capable of capturing keyed PAN and or SAD data on a merchant-controlled computing device.
Volume	A storage medium mounted on a Node or a Server. For payments, volume means total number of Transactions.

License Options

Each of the event-based license packages has three tiers: low, mid, and unlimited.

License	# Events ≤ 10M	10M < # Events ≤ 100M	# Events > 100M
Voltage SecureData Basic	Low	Mid	Unlimited
Voltage SecureData Standard	Low	Mid	Unlimited
Voltage SecureData Premium	Low	Mid	Unlimited

Unlimited Events Licensing: Based on the estimation of the number of events, the Unlimited Events SKUs are licensed for the entire duration of the subscription. The prices of the Unlimited Events SKUs are valid only for the duration of the subscription. There is no surcharge for consumption of events over the estimate within the duration of the subscription. Upon renewal, the events are re-estimated and priced appropriately for the next subscription period.

License	License Metric	Entitlement	Available encryption only	Available tokenization only	Available encryption and tokenization
Voltage SecureData Basic	Event	Data Privacy and Protection Foundation; Data Privacy and Protection APIs; Data Privacy and Protection Integrations	No	No	Yes
Voltage SecureData Standard	Event	Voltage SecureData Basic entitlements plus Data Privacy and Protection Payments	No	No	Yes
Voltage SecureData Premium	Event	Voltage SecureData Basic and Standard entitlements plus Data Privacy and Protection Sentry and Structured Data Manager	No	No	Yes

Voltage SecureData Basic

Voltage SecureData Basic licensing covers both cloud and off-cloud usage, and includes:

- Any number of Infrastructure Suites; Appliances and Clusters/Nodes/Pods; Datacenters; HSM Engines/Connectors; Named Applications; EDW or Hadoop Nodes; TB/PBs of Data; LBs/Gateways; Clients, Bundles, SDKs, Utilities, and Command Line tools; Cloud Integration Templates and Software; Developer Templates
- All types of Platforms (open systems, IBM Z, Hadoop, HPE NonStop, Stratus); Clients, Bundles, SDKs, Utilities, and Command Line tools; Environments (Production, Test, Dev, DR); Cloud Integration Templates and Software; and Developer Templates; Operations (Encryption, Tokenization/SST, Hashing, Masking)

Voltage SecureData Standard

Voltage SecureData Standard licensing covers both cloud and off-cloud usage, and includes, in addition to the entitlements of Voltage SecureData Basic:

- Any number of Payments POIs/Lanes; Payments Terminal/Mobile/Host SDKs

Voltage SecureData Premium

Voltage SecureData Premium licensing covers both cloud and off-cloud usage, and includes, in addition to the entitlements of Voltage SecureData Basic and Voltage SecureData Standard:

- Any number of Named Applications – Custom and SaaS; JDBC and ODBC Drivers and HTTP/Proxy Interceptors, and Database Instances

Software-Specific License Terms

Software products with software-specific license terms are described below. Software products covered by this ALA document (as listed above) and not covered in this section do not have software-specific license terms.

Legacy Voltage SecureData License Terms

SecureData Enterprise software as indicated in the table below is licensed in accordance with the following License Metric. Encryption or Tokenization can be licensed independently or together.

License	License metric	Available encryption only	Available tokenization only	Available encryption and tokenization
SecureData Enterprise Integrations to Cloud Services	Data Volume			Yes
SecureData Enterprise –Open Systems	Named Application or Gigabyte	Yes	Yes	Yes
SecureData Enterprise Data Warehouse (Non-Hadoop/Non-Cloud Service)	Node [2]			
SecureData Enterprise for Hadoop	Node [3]			Yes
SecureData for Snowflake	Data Volume [1]	No	No	Yes
SecureData for Stratus VOS	Named Application	Yes	Yes	No
SecureData Format- Preserving Encryption (FPE) for ArcSight Data Platform	Gigabyte [6]	Yes	No	No
SecureData z/Protect (IBM z/OS)	MSU	Yes	Yes	Yes
SecureData Protected Data Downstream Usage	Terabyte [7]			Yes

[1] Data Volume means the terabytes of data moved/ingested for storage/processing/use, and is either wholly or partially protected by Voltage SecureData.

[2] Node means, for Data Warehouse (Non-Hadoop/Non-Cloud Service), any computing Server where the Data Warehouse software is running and where SecureData APIs are deployed, and/or where data protected by SecureData is stored, processed or used.

[3] Node means, for Hadoop, any computing Server where the Hadoop software is running, and where SecureData APIs are deployed, and/or where data protected by SecureData is stored, processed or used.

[6] Gigabyte means the gigabytes (10^9 bytes) of data ingested by ArcSight per day.

[7] Terabyte means the volume of data measured in terabytes (10^{12} bytes) provided downstream, either wholly or partially protected by Voltage SecureData.

SecureData Enterprise use for Integrity NonStop Guardian or OSS is licensed per CPU.

SecureData Distributed Encryption Engine (Entrust nShield Connect or Atalla HSM Support) is licensed per Key Server.

SecureData Encryption or Tokenization for Network Gateways is licensed per Application for up to 1 million Transactions per year per annum as authorized in your order for the software (Authorized Transactions). If during the one-year period you exceed the Authorized Transactions, you are required to purchase additional Application licenses for the required total volume of Transactions. This license is not authorized to be used with SaaS Gateways.

SecureData Key Servers are licensed per Server.

SecureData Mobile Encryption is licensed based on the estimated annual volume of Transactions. Additional license(s) are required if the usage exceeds the annual estimated volume. Also requires infrastructure licenses along with the appropriate SecureData client software for the required platforms.

SecureData Protected Data Downstream Usage is licensed per Terabyte of total data, either partially or wholly protected by SecureData, and moved to downstream systems not otherwise licensed This license doesn't permit unprotecting protected data at those downstream systems.

SecureData Web Encryption is licensed based on the estimated annual volume of Transactions. Additional license(s) are required if the usage exceeds the annual estimated volume. Also requires infrastructure licenses along with the appropriate SecureData client software for the required platforms.

SecureData Web FES (Front End Server) is licensed per Server.

SecureData Web Services Servers are licensed per Server.

Legacy SecureData suites

Suite	Offering includes
SecureData Enterprise Data Warehouse Starter Edition	1 SecureData Key Server 1 SecureData Enterprise Web Services Server 1 SecureData Enterprise for EDW Installation Kit 1 SecureData Usage License for one Enterprise Data Warehouse Node [*]
SecureData Enterprise Data Warehouse Enterprise Edition	2 SecureData Key Servers 2 SecureData Enterprise Web Services Server 1 SecureData Enterprise for EDW Installation Kit 1 SecureData Usage License for up to 5 Enterprise Data Warehouse Nodes [*]
SecureData Enterprise Infrastructure Suite 1 – Production and Test and Development	2 SecureData Key Servers 2 SecureData Enterprise Web Services Servers 2 SecureData Key Servers for Test and Development Systems 2 SecureData Enterprise Web Services Servers for Test and Development Systems
SecureData Enterprise Infrastructure Suite 1 – Disaster Recovery	2 SecureData Key Servers for Disaster Recovery 2 SecureData Enterprise Web Services Servers for Disaster Recovery
SecureData Enterprise Infrastructure Suite 2 – Production and Test and Development Systems	2 SecureData Key Servers for Development Systems 2 SecureData Enterprise Web Services Servers for Development Systems 2 SecureData Key Servers for Test and Development Systems 2 SecureData Enterprise Web Services Servers for Test and Development Systems 2 SecureData Distributed Encryption Engine for Entrust nShield Connect **or Atalla HSM** 2 SecureData Distributed Encryption Engine for Entrust nShield Connect **or Atalla HSM** for Test and Development Systems
SecureData Enterprise Infrastructure Suite 2 – Disaster Recovery	2 SecureData Key Servers for Disaster Recovery 2 SecureData Enterprise Web Services Servers for Disaster Recovery 2 SecureData Distributed Encryption Engine for Entrust nShield Connect **or Atalla HSM** for Disaster Recovery
SecureData Suite for Hadoop Starter Edition	1 SecureData Key Server 1 SecureData Web Services Server 1 SecureData Enterprise Client Simple API and Client Installation Kit for Red Hat Linux Data Center 5 SecureData Hadoop Protection Encryption and Tokenization Nodes [*] 1 SecureData Hadoop Installation Kit
SecureData Suite for Hadoop Enterprise Edition	2 SecureData Key Servers 2 SecureData Enterprise Web Services Servers 2 SecureData Enterprise Client Simple API and Client Installation Kit for Red Hat Linux Data Center 20 SecureData Hadoop Protection Encryption and Tokenization Nodes [*] 1 SecureData Hadoop Installation Kit
SecureData Suite Open System Standard Edition – Test and Development	1 SecureData Key Server 1 SecureData Enterprise Web Services Server 1 SecureData Enterprise Client - Open Systems Bundle (Windows/Linux/Solaris/AIX/HP/UX/Mac OS X) Data Center - covers up to 500 GB of source data - limited to Test Data Management Use Cases only

Suite	Offering includes
SecureData Suite Open System Enterprise Edition – Test and Development	▪ 1 SecureData Key Server ▪ 1 SecureData Key Servers for Test and Development Systems ▪ 1 SecureData Enterprise Web Services Server ▪ 1 SecureData Enterprise Web Services Server for Test and Development Systems ▪ 1 SecureData Enterprise Client - Open Systems Bundle (Windows/Linux/Solaris/AIX/HP/UX/Mac OS X) Data Center ▪ covers up to 1 TB of source data ▪ limited to Test Data Management Use Cases only

[*] See software-specific license terms of SecureData Enterprise for definition of Node for Data Warehouse, and of Node for Hadoop.

Legacy SecureData clients

SecureData Enterprise Client Open Systems Bundle is licensed by Data Center.

SecureData Enterprise Client Simple API and CL Installation Kit is licensed by Data Center.

SecureData Enterprise Client Simple API for Linux on IBM Z is licensed by Data Center.

SecureData Host SDK Open Systems Installation Kit is licensed by Data Center.

SecureData Enterprise Client Hadoop is licensed by Data Center.

SecureData Installation Kit for Hadoop is licensed by Data Center.

SecureData Mobile Installation Kit for Enterprise/Merchant is licensed by Data Center.

SecureData File Processor is licensed by Data Center.

You are authorized to use and copy the SecureData client software and Installation Kits client software in object code form only solely to create Developed Code and to use and copy Developed Code solely for your internal use with the SecureData software. No rights to distribute the Developed Code are granted herein. You may make and use the number of copies of client software that you deem appropriate unless the number of copies of client software is restricted as set forth in the applicable order.

Legacy SecureData Mobile

SecureData Mobile software as indicated in the table below is licensed in accordance with the following License Metric. Encryption or Tokenization can be licensed independently or together.

Name	License metric	Available encryption only	Available tokenization only	Available encryption and tokenization
SecureData Mobile SDK	Transactions per Annum	Yes		

SecureData Mobile Infrastructure is licensed per number of Transactions per annum and by Data Center and limited to use for Encryption.

SecureData Mobile Add-on Infrastructure Suite for Acquirer/ISO/OEM (Service Provider) is licensed by Data Center and limited to use for Mobile. Base Infrastructure license needs to be included with this license.

Legacy SecureData Payments

SecureData Payments software as indicated in the table below is licensed in accordance with the following License Metric. Encryption or Tokenization can be licensed independently or together.

Name	License metric	Available encryption only	Available tokenization only	Available encryption and tokenization
SecureData Payments Base Infrastructure Suite for Acquirer/ISO/OEM (Service Provider) Tier1/Tier2/Tier3/Tier 4	Transactions per annum	Yes	Yes	Yes
SecureData Payments Encryption Add-on Infrastructure Suite for Acquirer/OEM/ISO (Service Provider) Tier1/Tier2/Tier3/Tier 4	Transactions per annum	Yes		Yes
SecureData Payments Tokenization Add-on Infrastructure Suite for Acquirer/OEM/ISO (Service Provider) Tier1/Tier2/Tier3/Tier 4	Transactions per annum		Yes	Yes
SecureData Payments Encryption for Point of Sale (POS) for Acquirer/OEM/ISO (Service Provider)	Lane	Yes		
SecureData Payments Tokenization for Point of Sale (POS) for Acquirer/OEM/ISO (Service Provider)	Lane		Yes	
SecureData Payments Encryption and Tokenization for Point of Sale (POS) for Acquirer/OEM/ISO (Service Provider)	Lane			Yes
SecureData Payments Encryption for Point of Sale (POS) for Enterprise/Merchant	Lane	Yes		
SecureData Payments Tokenization for Point of Sale (POS) for Enterprise/Merchant	Lane		Yes	
SecureData Payments Encryption and Tokenization for Point of Sale (POS) for Enterprise/Merchant	Lane			Yes

SecureData Payments Infrastructure for Encryption is licensed per number of Transactions per annum and per Data Center and limited to use for Encryption.

SecureData Payments Infrastructure for Tokenization is licensed per number of Transactions per annum and per Data Center and limited to use for Tokenization.

SecureData Payments Infrastructure for E-Commerce is licensed by Data Center and limited to use for E-Commerce.

SecureData Payments POS Connectors is licensed by Lane. This is the license that needs to be licensed in addition to the Infrastructure license.

Legacy SecureData Sentry

SecureData Sentry software as indicated in the table below is licensed in accordance with the following License Metrics.

Name	License metric	Available encryption only	Available tokenization only	Available encryption and tokenization
SecureData Sentry for Driver Interception	Application			Yes
SecureData Sentry for proxy interception	User			Yes

Legacy SecureData Web

SecureData Web software as indicated in the table below is licensed in accordance with the following License Metric. Encryption or Tokenization can be licensed independently or together.

Name	License metric	Available encryption only	Available tokenization only	Available encryption and tokenization
SecureData Web Add-on Infrastructure Suite for Acquirer/OEM/ISO (Service Provider) Tier 1/Tier 2/Tier 3/Tier 4	Transactions per annum	Yes	Yes	Yes
SecureData Encryption Use License for SecureData Web for Acquirer/OEM/ISO (Service Provider)	Transactions per annum	Yes		
SecureData Tokenization Use License for SecureData Web for Acquirer/OEM/ISO (Service Provider)	Transactions per annum		Yes	

Note: Encryption and Tokenization licenses for SecureData Web are listed under SecureData Enterprise.

SecureData Web is licensed based on the annual estimated Volume of Transactions. Add-on infrastructure for SecureData Payment Web is also required.

SecureData Web Add-on Infrastructure Suite for Acquirer/ISO/OEM (Service Provider) is licensed per Data Center. Payments Base Infrastructure license is also required.

SecureData Web Infrastructure is licensed by number of Transactions per annum and per Data Center and limited to use for Encryption.

SecureFile

SecureFile is an Add-on to SecureMail and is licensed by User and by Application; when licensed by Application a minimum of 50 Users must also be licensed.

SecureMail

SecureMail Application Edition is licensed by number of Applications.

SecureMail Essentials Edition is licensed by User.

SecureMail Standard Edition is licensed by User.

SecureMail Enterprise Edition is licensed by User.

SecureMail Edition Upgrade is licensed by User.

SecureMail Mobile Edition is licensed by User.

SecureMail Statements Edition is licensed per the number of Messages per annum as authorized in your order for the software ("Authorized Messages"). If during the one-year period you exceed the Authorized Messages, you are required to purchase additional licenses for the required total volume of Messages.

SecureMail for BlackBerry Dynamics is licensed by User.

SecureMail for BlackBerry Enterprise Server Add-on is licensed by User.

SecureMail for Symantec Enterprise Vault Add-on is licensed by User.

SecureMail eDiscovery Accelerator Add-on is licensed by User.

SecureMail Large Attachment Delivery Add-on is licensed by User.

SecureMail for Remote Desktop Services Add-on is licensed by User.

SecureMail Connector for Entrust nShield Connect Add-on is licensed by User.

SmartCipher

SmartCipher software as indicated in the table below is licensed in accordance with the following License Metric.

Name	License metric
SmartCipher Data Protection Suite for Endpoint Sensor	Per Device

Structured Data Manager

Structured Data Manager (SDM) is used by global organizations to address critical business requirements including:

Structured Data Manager capabilities and benefits

Capability	Description
Discover sensitive data	Automatically discover sensitive data across all repositories.
Protect sensitive data	Apply masking and Format-Preserving Encryption to structured data.
Comply with data privacy laws	Regulatory compliance is evolving to include requirements for data protection, data subject access rights (DSAR), and the right to be forgotten. SDM can address these use cases across the enterprise.
Increase operational efficiency	Expedite backup performance and accelerate disaster recovery.
Lower total cost of ownership	Reduce your data footprint and storage costs, including hardware, maintenance, and administration.
Provide federated data access	Increase data accessibility with simultaneous access to production and archived data, using combined reporting.
Test Data Management	Protect and generate test data for QA, Dev and Testing groups
Data Privacy Management	A bundle containing SDM core, Discovery and the ability to apply format-preserving encryption/decryption.

Structured Data Manager is licensed by Source Database. If multiple Databases exist on one physical Server, each Database to be archived/extracted/processed is considered a Source Database and must have a separate license. For example, if three Databases reside on one physical Server and only one will be archived with Structured Data Manager, only that one Database is considered a Source Database and requires a license. Licenses cannot be transferred between production Databases.

Structured Data Manager Single Source Platform: includes the license-to-use (LTU) for archiving data from a production Database to an archive in either the form of another Database or a file. Licensing is determined by:

▪ The number of production Database instances where data is sourced from, if multiple Databases exist on one physical server, each Database acting as a source must have a separate license. For example, if 3 Databases reside on one physical server and only one will be the source of Structured Data Manager, only that 1 Database requires a license.

Licenses cannot be transferred between production Databases.

Database Activity Monitoring (Voltage Database Activity Monitoring)

Database Activity Monitoring software as indicated in the table below is licensed in accordance with the following License Metric: Server and Database Server

Name	License metric
Database Activity Monitoring Server	Unit
Database Activity Monitoring Database Server	Database Server

Database Monitoring Server Is licensed by a Unit. Each independent installation of Database Activity Monitoring is required to have a license for a Database Monitoring Server.

Database Monitoring Database Server is licensed by Database Server. Each Database server being monitored by Database Activity Monitoring is required to have a Database Activity Monitoring Server license per Database.

Additional License Terms

	Term
A.	Any licensing terms designated as being of Voltage Security Inc. that may be embedded in the software are inapplicable in their entirety.
B.	Software contains software and associated specifications licensed from third parties that are confidential to, and trade secrets of, such parties. You will not take any action other than to Use it as authorized under the agreement as part of the software products and will not disclose it to third parties.

Additional License Authorizations

For OpenText™ Data Privacy and Protection software products