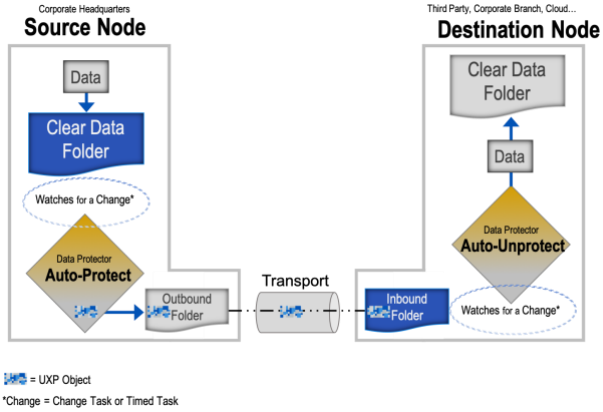
Data Protector DATASHEET

The Sertainty Data Protector (DP) is an independent process that stands alone for protecting and accessing data targeting the machine-to-machine business data flow. The DP performs automated UXP Technology Tasks within the existing data flow customized to the security needs of the data as defined by the owner. It does not require integration with existing software applications or data process flows; the DP facilitates the creation and accessing of protected UXP Objects and functions in most environments (see Platforms).

Using the Data Protector, data owners can define and assign UXP Tasks suited for their specific data flow. The DP operates on the surface as a Task Manager and collaborates with a process running in the background, the Sertainty UXP Agent. The Agent schedules and monitors the UXP Task activity for execution as well as other technical functions for the DP.



UXP Tasks are the technical instructions configured for the automated processes *Auto-Protect, Auto-Unprotect* and *Compliance Monitoring*. Two Task types exist: *Change Task* and *Timed Task*. Included in a single task are: an executable (*predefined proprietary UXL Script* or *custom program*), folder locations and other required script parameters for Task execution. Once UXP Tasks are configured, the Data Protector facilitates the Task action, and the Agent executes the script for the DP automated process. All other processes within the data flow are managed by the existing software or applications.

BENEFITS

- Seamless leverage of Sertainty UXP Core Technology using the SDK
- Data-centric
- Self-governing controls are defined by the UXP Identity (see UXP Identity info sheet)
- Non-invasive integration with existing applications and data transfer processes. No code changes are required
- Utilizes existing data transport process
- Auditing capabilities
- Notification capabilities

PLATFORMS

- 64-bit Linux (Ubuntu, Oracle, AWS, CentOS, Fedora, Redhat) – kernel 3.10.0-957 and above
- Currently supported VM hypervisors:
  - VMware
  - VirtualBox
  - Additional versions in test
- 64-bit Windows
- macOS
- Unix is feasible; system is built using C++ and standard libraries

FEATURES

- Sertainty Agent, configuration is managed as an *.xml file
- DP process is defined as either:
  - Change Task– watches a folder for changes and processes new files
  - Timed Task– executes the action based on a scheduled interval
- Executable can be created using:
  - UXL Script Engine (*.uxl)
  - Native binary or native script (*.exe, *.bat, *.sh., etc.)
- Configurable:
  - Number of files included in each UXP Object
  - File types
  - Log file generation

RESTRICTIONS

- Machine to machine workflows
- Each DP Task runs as a separate thread
- Mobile currently not supported
- Rulesets for compliance require manual design and updates

DISK SPACE

- 626 MB macOS
- 291 MB Windows
- 279 MB Oracle
- 242 MB Ubuntu

MEMORY REQUIREMENTS*

- 83 MB macOS
- 126 MB Windows
- 279 MB Oracle
- 242 MB Ubuntu

*Actual run time is machine dependent

AUTO-PROTECT

The Auto-Protect process using a predefined UXL Script executes automatic UXP Object (Object) creation. The Data Protector facilitates the process by using the UXP Identity (UXP ID) that is locked to the Destination Node to convert clear data to an Object. The UXP ID travels covertly embedded in the Object and contains the access parameters to extract data, but also actively participates in securing the data in any location.

Utilizing a configured folder structure, the DP with its assigned UXP Task executes the process on the Source Node. Three defined folders are needed with definitive locations (generically titled here): Source Clear Data, Outbound and Source Log. The Source Clear Data is the "watched" folder where processed clear data with specified file extensions on the Source Node awaits UXP Object conversion. The DP looks only for those file types in that folder and then generates the UXP Object. Once created, the DP places the UXP Object in the Outbound folder ready for transport. This folder may already exist in the data flow, but the DP requires a defined folder to complete the Auto-Protect process. The Source Log houses the generated UXP Log Files. Each UXP Object created has a corresponding log file for tracking the DP activities on the Source Node. The Log Files are protected using UXP Technology and undisputable, but can be accessed by the data owner.

The Auto-Protect Task can be configured to convert a single file to one UXP Object or for many files to one UXP Object.

AUTO-UNPROTECT

The Auto-Unprotect process operates on the Destination Node using a predefined UXL Script for automatically accessing and extracting data from a UXP Object. The UXP ID used to protect the data on the Source Node is based on the Destination Node's unique digital fingerprint. During the configuration of the Destination Node, the Data Protector simultaneously behind the scenes generates the associated UXP ID and stores it locally in a special UXP file format. In this location, the UXP ID is used during authentication to determine trust for data access and extraction. To be used to protect data, the Destination Node's UXP ID is provided on the Source Node.

Like the Auto-Protect, the Auto-Unprotect process requires a similar folder configuration to execute its assigned UXP Task. The three folders with definitive locations (generically titled here) are: Inbound, Destination Clear Data and Destination Log. After transport from the Source Node, UXP Objects arrive in in the Inbound folder, which as noted above may already exist in the data flow, serves as the "watched" folder for the DP. The DP looks only for incoming Objects. When an Object is detected, the Data Protector, as a facilitator, initiates the Auto-Unprotect Task to attempt to access the protected data. The Object, carrying the UXP ID locked to this Destination, activates and assesses the local environment. The UXP ID associated with this Destintion Node must match identically to the UXP ID with the Object for access and extraction to occur. Otherwise the Object remains protected. The DP places extracted data contents in the Destination Clear Data Folder for the existing applications to continue processing. The Destination Log Folder houses the UXP Log Files tracking access and extraction in the same manner as the Object creation Log Files on the Source Node.

COMPLIANCE MONITORING

Archiving UXP Objects involves using the Auto-Protect process with the protected data being delivered to a cold storage. A Timed Task is configured for the Data Protector to manage. A UXP ID is generated for a Destination Node that it used to access archived Objects. That UXP ID, with rules and parameters for compliance timelines, will be used to create the Objects.

With Compliance Montoring, the process routinely checks compliance dates on Objects. When a timeline is met, the Object is moved to the Destination Node where it is authenticated and accessed and the data is shredded.

In the current, Data Protector version, Compliance Monitoring is limited.

Email us today:
tech-support@sertainty.com