UXP Technology Technical Overview

Sertainty UXP Technology (UXP) focuses on protection at the data layer targeting any kind of unstructured datasets (excluding databases). UXP empowers data to manage and protect itself by controlling access anywhere and at any time.

UXP combines intelligence, protection and user datasets to transform data into a self-governing, self-protecting entity capable of enforcing owner-specified access controls or parameters and context. The transformation result is a UXP Object.

The UXP Object is a self-contained, uniquely protected entity capable of managing and controlling its own access to ultimately keep its content protected in any location. In this format, it is an intelligent entity that acts on behalf of the data owner once the secured dataset has moved beyond the owner's environment. The data control remains with the owner at all times and is never relinquished to an application nor vulnerable to super-user access.

UXP Object rendition

Transformation:

Embedding Intelligence & Protection

During data's conversion to a UXP Object, Sertainty UXP Technology essentially mixes proprietary UXP Metadata incorporating intelligence and protection artifacts with the dataset. Once generated, the mixed artifacts and dataset are now cloaked and distinctly protected in the Object.

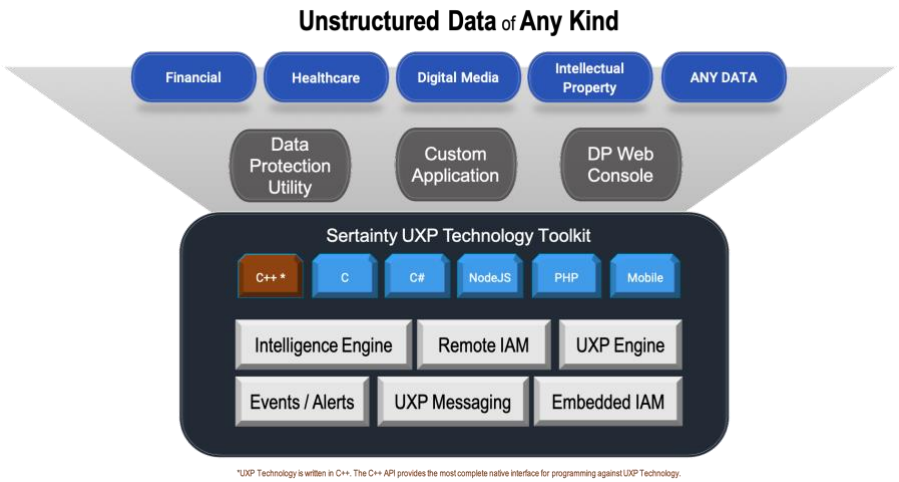
The intelligence is a proprietary executable called the KCL Program within the Object. It provides the Object with functionality for policy enforcement and self-auditing. It also equips it with the ability to establish an irrefutable record of ownership and to track access activity without deviation. The protection is a unique scheme that includes AES256-GCM encryption methodology plus added proprietary algorithms that don't require a separate key sharing process. Keys are created during the conversion process and are managed internally by the UXP Object. The intelligence and protection now mixed with the dataset are embedded unseen in a UXP Object and travel as one entity appearing as an inert binary file only recognizable by UXP Technology Libraries.

Access Controls:

UXP Object Ruleset

The access controls or parameters are fundamental in UXP Technology. They participate directly in the generation process for the protection scheme of a UXP Object and actually become part of the protection scheme itself. These protection parameters are defined by the data owner based on the security needs of the data, its environment and how it moves. They are referred to as an access ruleset that the UXP Object via the KCL Program directly references to actively manage and control access.

They can consist of a single parameter, a designated machine where the dataset can solely be accessed, or multiple parameters customized to suit specific circumstances (i.e. compliance in health or finance industries). Once created, the ruleset is protected in a separate special UXP entity called the UXP Identity (UXP ID). Additionally contained within the UXP ID is a machine profile with its associated unique digital fingerprint. This fingerprint is a random collection of machine identifying attributes that irrefutably ties it to a single machine that is permitted to access the dataset.



Architecture

UXP Technology has modular architecture and supports multiple platforms including Windows, Linux and macOS.

UXP Technology also provides a comprehensive library that includes a set of powerful APIs. It allows the Technology's self-protecting data functionality to be instrumented within custom software such as workflows, machine to machine data processing, or any application that requires total privacy for the provided access control list.

Using the native API written in C and C++, a developer can take full advantage of the Technology by giving applications direct access to protected data without worrying about encryption or decryption. Applications can read and write data using basic I/O calls that resemble standard calls in the C standard library. Advanced operations, such as directory management, document-level access control and signatures are also supported by the API. Additionally, a C-like native scripting language permits development of utility scripts, batch scripts and advanced workflow operations.

The UXP Technology Libraries are user-mode libraries that don't require special privileges to use.

Implementation & Functionality

The UXP Technology Libraries are implemented on the machine where clear datasets are to be converted to UXP Objects as well as on the machine where the UXP Objects are to be accessed. Depending on the data flow, the implementation may be a single machine or many. The UXP Object creation and access configurations are designed based on the existing data flow and the needed protection parameters for the data. Once configured, the processes execute seamlessly within the existing flow.

Required in the conversion process is the UXP ID. Functioning together with the Libraries, the ruleset, machine profile with additional UXP Metadata and the dataset are uniquely mixed and transformed into a UXP Object.

When the UXP Object resides in its designated machine location where UXP Technology Libraries are also present, the Technology is able to accurately identify it. The UXP Object is "activated" and the KCL Program immediately assesses its environment. It compares the environment to its embedded ruleset and unique machine digital fingerprint to determine trust. The details MUST match exactly for trust to be fully established before UXP Object authentication occurs. If trust is not established, then the UXP Object will actively prevent authentication.

Email us today:
tech-support@sertainty.com