XTINCT: Secure Data Destruction
A Compliant Data Erase Tool for z/OS Disk & Tape Data

XTINCT Introduction

XTINCT is a tool for wiping data from z/OS originated DASD and tape to ensure the original data is unrecoverable and therefore unusable. The product provides users with various levels of protection to ensure compliance with all global industry, security, government, corporate and regulatory compliance requirements, for example, Basel II, DoD, European Data Protection Directive, Gramm-Leach-Bliley HIPAA, Payment Card Industry Data Security Standard, Sarbanes-Oxley, naming but a few…

Why is XTINCT Required?

Historically, disk or tape media was accessed by only a few people, password protected and considered reasonably safe and therefore secure. Even Disaster Recovery (DR) testing at offsite locations didn't raise much concern for the safety of corporate data. After such testing, it was typical to scratch the disk Volume Table of Contents (VTOC) and leave the DR testing facility thinking that sensitive company data was safe. Clearly today, data security is a different story!

Terrorism, identity theft, off shoring, outsourcing, litigation, the Internet and the global economy have all highlighted the need for increased data protection. Governments have passed legislation to hold corporations responsible for securing private information under their care. Beyond government standards, industry regulations such as the Payment Card Industry Data Security Standard have further defined the rules, and corporations desiring to do business with them must be in compliance. Failure to comply with these standards for data protection can result in large business losses and severe penalties; so it is no longer simply a matter of due diligence to protect data under your control, it is a necessity!

XTINCT Functionality Overview

XTINCT provides DSF/E (Device Support Facilities/Extended) functionality, which supplements the basic function provided by the standard DSF facilities provided by IBM, typically known as ICKDSF. In addition to providing a complete audit trail and comprehensive reports to satisfy regulators, XTINCT surpasses NIST guidelines for 'cleaning' and 'purging' data. XTINCT also satisfies all federal and international requirements including Sarbanes-Oxley, HIPAA, HSPD-12, Basel II, Gramm-Leach-Bliley and other data security and privacy laws. The primary functions and associated benefits of XTINCT are:

- XTINCT is re-entrant and fully supports sub-tasking. Multiple volumes can be processed asynchronously. Other tools, like ICKDSF, run serially.
- XTINCT makes extensive use of channel programs. Many functions operate at peak efficiency by only using enough CPU time to generate the channel programs, with the rest of the operation being carried out by the channel subsystem. This makes XTINCT a very efficient utility, utilizing minimal CPU resources.
- Control statements allow for PACING the number of concurrent operations against a string using the TASKMAX parameter. The user can run one task or many at the same time.
- XTINCT provides four levels of erasing data to satisfy even the most demanding requirements.
- XTINCT provides a pattern write that reverses each bit (I.E. one's compliment) to eliminate the possibility of reading residual data.
- To safeguard that the data pattern is written to disk, XTINCT forces the storage controller to destage all modified tracks at the end of each pass and prior to starting the next one. This precludes a second pattern replacing the first pattern in cache and never being written to the disk, while still making efficient use of NVS and cache.

Are There Zero Cost Options Available for Data Erasing?

There are no reliable zero cost or "Freeware" options for secure z/OS data erase activities With the standard supplied utilities such as IEHPROGM, individual data sets or the entire VTOC can be scratched. However, that simply removes the pointer to each data set, leaving all the data on the disk. ICKDSF can perform a MINIMAL INIT to create a label and a new VTOC, but this also leaves all the data on disk. A MEDIAL INIT will re-write the Home Address and record zero, but may still not render data unreadable. Consequently, it will not satisfy the required standard for clearing or purging data. Furthermore, these techniques also take a very long time! Clearly data security requires a robust tool that erases data to exacting standards, as quickly as possible, minimizing data security exposures and maximizing technical personnel and CPU optimization efficiencies.

Value-4IT Limited
7 Wright Road, Long Buckby
Northampton, NN6 7GG
United Kingdom
Tel: +44 (0) 845 0579386
sales@value-4it.com
www.value-4it.com

Dino-Software Corporation
P.O. Box 7105
Alexandria, VA 22307
United States of America
Tel: +1 703 768 2610
sales@dino-software.com
www.dino-software.com