QUIKPROTO

TrustedDoc

Enterprise Digital Rights Management

Incubated Under
Electropreneur™
PARK

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

MEMBER
NASSCOM®
MEMBER

Introduction

TrustedDoc: is an enterprise scale Digital Rights Management (DRM) platform developed ground up to provide a systematic approach to copyright protection for digital contents. The solution prevents unauthorized redistribution of digital contents and restricts the ways consumers can copy cut or paste the contents of a document. The solution provides protection through hybrid military grade encryption which can be accessed using its unique multi-tiered authentication methods. The User can view only the document assigned to him with DRM Policies applied on it. In case the document gets leaked in any way it can be tracked since the document will be dynamically watermarked with IP, Date, Time, User ID. The system has been used by ISO and evaluated by the Army.

Distributed document usage control

This allows information which is generated and distributed to be controlled centrally. TrustedDoc allows control of intellectual property to be retained even after the information has been shared with another person / company. For example it is possible for a person to send a document containing his personal details to his legal / financial advisor and after getting the advice ensure that all copies of the same document are destroyed or rendered unprintable afterwards. It is also possible to restrict the use of information for viewing, printing, and forwarding based on time and location. For example, an information is viewable only by Mr.X till Monday and cannot be further shared by him, cannot be printed by him, and cannot be downloaded to his system.

Features & Benefits

01

Supports most dominant document formats

TrustedDoc supports most dominant enterprise document formats like doc, xls, ppt, pdf, txt, gif, jpg, bmp, jpeg etc. This is an ever-growing list as we release more and more documents format support.

02

Protects documents within & outside of the enterprise

Documents can be configured and used within the enterprise as well as outside for customers and partners. This means no restrictions for valid document usage.

03

Controls who, what, when & where.

Controls who (people, groups, teams,...), what (read, print, distribute,...), when (dates) and where (locations, IP addresses, ...) can use the documents.

04

Full audit of authorized & unauthorized activities

Central availability of the audit trail of all activities on the document ensures that deviations can be caught early on as well as compliance to regulatory frameworks is easy to ensure.

05

Dynamic usage policies

Document usage policies can be changed even after distribution and can constantly reflect business status and relationships i.e. documents shared with vendors can be remotely destroyed once the time is over.

06

Web based administration

Administrative functions like user & file rights management, compliance reports etc. can be performed using a web based interface.

Typical usage control problems faced by organizations

As enterprises become more and more distributed, the need to control usage of information across the enterprise is increasing. Typical problems faced are

1. Information misuse:

Information shared with employees and business partners is frequently misused. The challenge faced by most enterprises is defining the (increasingly thin) line between legitimate use and misuse. Information shared with employees is frequently edited and distributed by them. In quite a few cases the editing and distribution is misused though the person himself might be a legitimate user of the information.

2. Internal information theft:

Stolen laptops, corporate espionage and employees joining competition are increasingly costing businesses by way of information loss

3. External information theft:

Even if the organization itself takes measures to control the information flow, misuse and leaks still happen when this information leaves the enterprise boundaries. Customers and vendors contribute to an increasing number of information thefts for organizations.

4. Managing collaboration with security:

Most IT administrators would accept the fact that achieving collaboration whilst maintaining security of digital information is a tough task. As different means of collaboration increases (via email, removable media, IM, web portals), the conduits for information leakage also increases. Thus, one suffers at the cost of the other.

5. Monitoring & regulatory compliance:

With the distributed nature of operations within and outside of the enterprises, compliance to digital asset management policies of regulatory frameworks means not only internal compliance but also compliance of the value chain of partners, vendors and customers. Given that most information is in the form of documents, this activity is nearly impossible with the present systems.

MEMBER NASSCOM® MEMBER

DSCI PROMOTING DATA PROTECTION A NASSCOM® Initiative

Incubated Under Electropreneur™ PARK