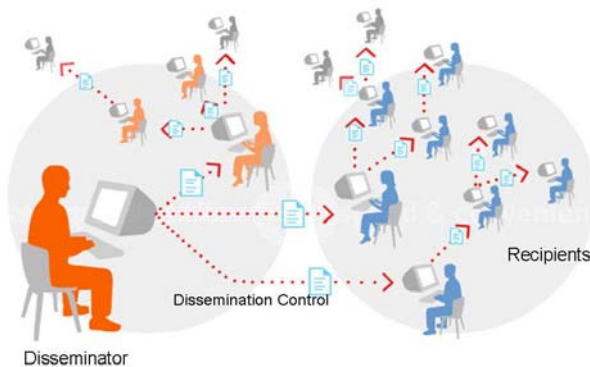




# Trusted Document Controls (TDOC)

## Flexible Policy Models and Architecture for Client and Server-assured Document Access Controls



### Overview

The TDOC research project underway at SPARTA and EMC addresses an increasingly important problem faced by the intelligence community (IC) as it moves towards the “need to share” paradigm. In essence, how can the IC enable controlled sharing of electronic documents to enable collaboration and yet not lose control over electronic disseminations? The TDOC project is developing advanced models and prototypes for controlling the access and dissemination of digital documents and the subsequent auditing, tracking, and analysis of redisseminations.

This research is sponsored by the Intelligence Advanced Research Projects Activity (IARPA), formerly Disruptive Technologies Office (DTO), as part of the initiative on “Advanced Countermeasures for Insider Threat” (ACIT). The project is currently in Phase 2 and developing an advanced prototype in collaboration with the EMC Corporation. It will integrate with backend document management systems and online directories to enable deployment in pilot programs within the intelligence community (IC). Dissemination control and analysis schemes are crucial preventive technologies for mitigating insider risks associated with document leaks.

### Motivation and Value Proposition

The motivation behind TDOC-style advanced dissemination control (DCON) technology comes from the realization that neither discretionary nor mandatory access controls (DAC and MAC) provide an adequate solution to flexible information sharing of digital content such as electronic documents. In particular, DAC and MAC models do not recognize the notion of “copies” of content and are further not good at tracking and controlling the usage and dissemination of copies. Also, these models are not aligned to accountability-aware workflow processing.

With emerging forms of digital content, the duplication and redissemination (through email, Internet and ftp downloads etc.) are easy. Thus, new models and enforcement controls are needed to address these challenges. In our TDOC DCON models, redissemination is modeled as a fundamental primitive. This enables document users to specify, control and track redissemination chains that span multiple recipients and systems. These may fan out as trees and graphs.

TDOC style technologies will significantly enhance the capability of the IC to share content by specifying a rich set of flexible policies for sharing, after delivery control and tracking.

### Technical Approach

The TDOC project is pursuing two directions that will combine to enable revolutionary advances and rapid technology transfer to the intelligence community.

#### (1) Models for dissemination control

First, we are developing advanced models for dissemination control (DCON). Our DCON models support a policy-based framework for the modeling and specification of a rich set of redissemination and usage controls. The models also enable dissemination analysis, i.e. the

tracking, auditing and analysis of redissemination, access and usage.

**(2) Use of commercial DRM technology**

Second, to enable rapid transfer, the TDOC prototype is being built on commercial digital rights management technology from EMC

Corporation. Documents are always encrypted at rest and also disseminated in encrypted form. A document is decrypted and rendered at a client machine only if a user satisfies certain dissemination, access control and usage policies. This commercial DRM platform is already in use within the IC.

**Architecture of TDOC-DCON Prototype**

