

# Rationale and impact of removing “offline salvage” issue from P2600 PPs

---

*Brian Smithson, Ricoh Americas Corporation, 6/16/08*

## **Background**

Since 2004, we have been trying to create a threat definition, objective, and requirements, to protect document data from being salvaged from hard disk drives that have been removed from HCDs. We have assumed that the requirement would typically be fulfilled by a combination of encryption (for live data) and overwrite (for deleted data).

## **Previous approaches**

To avoid the possibility of implying a requirement that all HCDs must have nonvolatile document storage, we placed the threat, objective, and requirements in a separate PP (within the family of PPs) that must apply when nonvolatile storage is present in a conforming product.

To avoid the possibility of implying that this requirement applies to nonvolatile storage that could not reasonably be removed from an HCD for salvage (for example, small flash or other nonvolatile memory devices that are embedded in the controller), we have used language like “devices that can be practicably removed”.

Until recently, we have used FDP\_RIP to require overwrite, and FCS\_COP to require encryption.

## **Current approach**

The current draft relies on the common PP threat and objective to protect document data from unauthorized disclosure, but puts the requirement to protect data from offline salvage in a separate “NVS” package.

We have discovered that the use of FDP\_RIP is inappropriate if we expect that it will be satisfied by overwriting. Also, we had previously discovered that selective overwriting is not a solution that works on flash memory devices and some hard disk devices that reallocate logical-to-physical mapping based on wear level, errors, or other factors that are beyond the knowledge or control of the TSF.

Specification of FCS\_COP has been a problem because (a) encryption is an implementation technique, and (b) FCS\_COP is not intended to require encryption, it is intended to establish requirements about how encryption is performed and managed.

Therefore, we proposed to apply FDP\_UCT in an unusual way to require protection from unauthorized disclosure of user data. We have done so by interpreting “export” to mean removal from the TOE, and “transmission” to mean storage on a device that can be removed. For consistency, we have also proposed to apply FTP\_ITC in a similarly unusual way to protect TSF data.

## Rationale for removal

### Out of scope for Common Criteria SFRs

Common Criteria SFRs fulfill objectives by requiring actions of the TSF in an operational. There are no SFRs that require TSF actions which protect assets when the TSF itself is not operational. In other words, CC assumes that the TSF is up and running when the threat is present. However, we have been trying to use SFRs to establish requirements that protect assets when the TSF is powered off and when those assets have been removed from the TOE.

### No satisfactory solutions have been found

Not surprisingly, we have been unable to identify SFRs that address this kind of situation in a straightforward, understandable manner. Our previous approaches have been found to be unusable, and recent comments indicate that the current approach is not understandable.

### Inconsistent with other similar IT products

Other IT products that are certified in the EAL2 – EAL3 range do not address offline salvage issues, even though many of those products handle similar assets in similar environments. Why should HCDs address this issue when other IT products in the same information flow (e.g., users' PCs, file servers, and print servers) do not?

### Limited value

There is a legitimate purpose for preventing offline salvage when an HCD (or any other IT product) is decommissioned or redeployed. Typical methods would involve full disk overwrite, degaussing, or even physical destruction. This has not been the intention of P2600 PPs.

In all environments, we have assumed that the HCD is in a secure or monitored area that protects the HCD from unauthorized physical access. If that assumption is not upheld in a customer environment, then all bets are off: a malicious user could do a variety of things that would compromise the security of document data, and removing a hard disk is just one example.

## Changes required to remove

### Eliminate NVS package from all environments

If we agree to remove this issue from the P2600 PPs, it is very easy to accomplish in the PP+packages structure. We only need to remove references to the NVS package from the common PP and remove the NVS package itself. There is no change to assets, threats, objectives, assumptions, policies, or requirements in the common PP.

### Remove or change compliance subclauses in IEEE Std. 2600

For consistency, we would need to amend the approved standard 2600 to remove compliance clauses 8.1.1.4, 8.1.2.4, and 8.1.3.2. Alternatively, these clauses could be retained if they are changed from "shall" to "should" (similarly to how we handled DoS attacks, as in clause 8.1.1.11).

## Impact of removal

### **Residual data is still protected, but in the traditional manner**

The current drafts apply FDP\_RIP in a traditional manner to both volatile and nonvolatile storage. This means that residual data cannot be accessed by normal system interfaces. This should satisfy the most recent comments from NIAP.

### **STs can still specify and satisfy requirements to protect data from offline salvage**

If we remove this issue from the P2600 PPs, vendors can choose to add requirements for protecting data from offline salvage. They will face the same issues that we have faced in the PP, but they will benefit from being able to design their solution to suit a particular implementation.

STs may approach this issue in ways that are dubious (e.g., FDP\_RIP) or undesirable in a PP (e.g., extended component definitions), and still get certified. However, I do not think that we should codify it in the P2600 PPs and burden all future ST evaluations with such an approach.