NIAP Policy #28 Implementation Guide

March 8th, 2021

National Information Assurance Partnership's (NIAP's) Common Criteria Evaluation and Validation Scheme (CCEVS) Policy #28 allows the construction of Composed TOEs (and the ability to perform evaluations of such TOEs) using an already-evaluated Distributed Security Component (DSC; evaluated against the DSC collaborative Protection Profile (cPP)) TOE along with the *dependent technology* (for example, a mobile device as specified in the Mobile Device Fundamentals (MDF) PP). As indicated in Policy #28, a NIAP-approved PP that specifically accounts for the use of a DSC is referred to as Approved Dependent Technology PP. Approved Dependent Technology PPs are identified in Appendix A to this implementation guide.

This document provides guidance on the production and use of documentation from the DSC and dependent technology evaluation efforts, and the activities that need to be performed in order for the evaluation of the "Composed TOE" to be accepted by NIAP.

Overview and Terminology

The purpose of Policy #28 is to allow product evaluations where the product being evaluated makes use of the capabilities of an evaluated DSC TOE so that those capabilities do not have to be re-evaluated. The DSC is a hardware and firmware TOE that exports a set of functions that has been evaluated against the DSC cPP. These functions are specified in the DSC's ST, and are referred to in this guidance as the **Supported Services Catalog**. The Supported Services Catalog corresponds to the information specified in the DSC cPP Supporting Document, section 5.2.1.4. The relationship between the DSC and the Dependent Technology is illustrated in Figure 1.

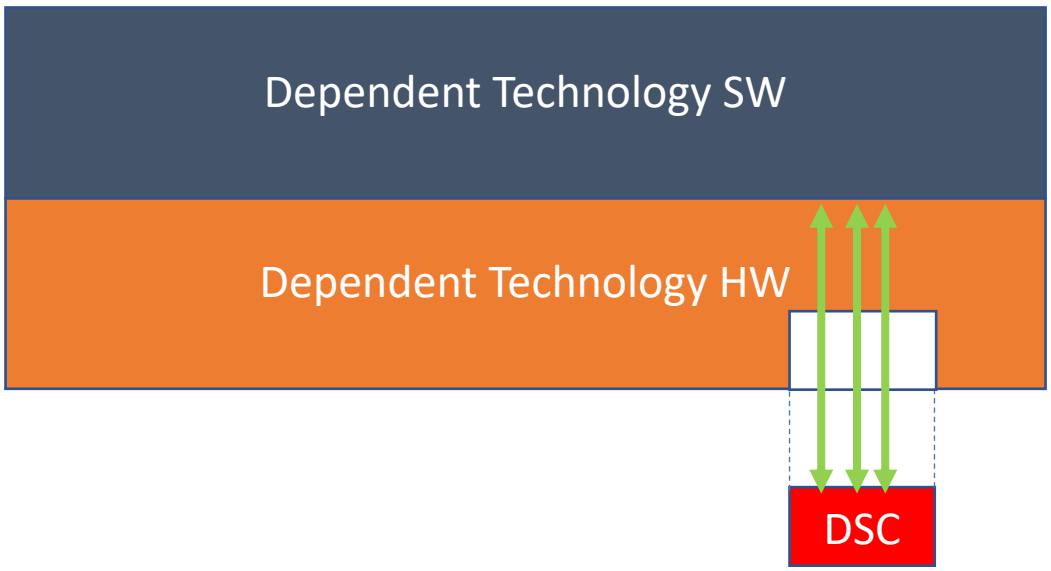

Figure 1 : Composition Model

In Figure 1, **Dependent Technology** refers to the product that invokes DSC functionality to satisfy some of its SFRs. In this document "Dependent Technology" is often used to indicate the functions of the Composed TOE that are not performed by the DSC.

Dependent Technologies that are suitable for use with Policy #28 will be specified in Appendix A of this document. From a practical standpoint, these technologies will correspond to Protection Profiles, and so the following guidance uses the terms:

- **Approved Dependent Technology PP:** A protection profile that has been written to allow DSC functionality to satisfy some or all of its requirements, and that is listed in Appendix A of this document.
- **Composed TOE:** The TOE that will receive the certificate as a result of evaluation against the Approved Dependent Technology PP and incorporates the evaluated DSC TOE. Put another way, this is the TOE that is described by the ST that is conformant to the Approved Dependent Technology PP.

The basic approach to evaluation of a TOE against an Approved Dependent Technology PP is that the PP will specify evaluation activities for all of its SFRs, and will also explicitly identify those SFRs that may be satisfied by a DSC TOE (this is what distinguishes an Approved Dependent Technology PP from a "normal" PP for that technology). To allow significant flexibility, the Approved Dependent Technology PP will have Evaluation Activities specified for all of its SFRs, including those that may be satisfied by a DSC TOE. The Composed TOE ST will indicate which of these functions are actually satisfied by the particular DSC instance used in the Composed TOE, and then the EAs (in the Approved Dependent Technology PP) associated with those functions will not have to be performed; the activities specified in this guidance will be performed instead.

DSC Evaluation and Evidence

In order for the composition approach to be successful, evidence from the DSC evaluation must be made available for the Composed TOE evaluation. This evidence must be available to any Common Criteria Test Laboratory (CCTL) that is performing the evaluation of the Composed TOE against an Approved Dependent Technology PP, where the CCTL performing the evaluation may be different than the one that performed the DSC evaluation. The details of this information are specified in the DSC cPP, specifically in the construction of the Supported Services Catalog (DSC SD section 5.2.1.4). This catalog includes the interfaces exported by the DSC that can be used by the dependent technology (and associated inputs and outputs); and an indication of which aspects of the interfaces were evaluated (for example, a crypto interface may provide many different services by crypto algorithm and mode, bit length, etc., but only certain combinations may be valid for the evaluated configuration of the DSC). As indicated previously, the DSC and Approved Dependent Technology PPs will identify interactions at the SFR level, and so a specific DSC evaluation will produce the interface information that will be used by the evaluators of the Composed TOE.

It is acceptable to evaluate multiple models of a DSC product in a DSC evaluation, including equivalence considerations as allowed by the DSC cPP. However, in order to perform evaluations according to Policy #28, each model will need to clearly indicate the Supported Services Catalog that it provides. Any model not specifically listed in the DSC TOE's ST will not be eligible for use in a TOE evaluation for an Approved Dependent Technology PP.

While in most cases the DSC will be evaluated prior to the evaluation of the Composed TOE, it is also permissible for the DSC to be evaluated concurrently with the Composed TOE. The outputs are no different, but the timing of the evaluation activities will need to be managed in order for all of the guidance outlined below to be followed (for example, the list of supported services from the DSC will have to be identified prior to identifying the requirements in the Application Dependent Technology PP that will be satisfied by the DSC for the Composed TOE). Further, the CCTL will have to manage risk where a DSC evaluation activity may prove to be unacceptable, and thus impact the ability to complete the Composed TOE evaluation.

Dependent Technology Requirements Specification

An Approved Dependent Technology PP is a PP that has been constructed so that the PP identifies SFRs that can be satisfied by functions provided by the DSC, similar to the model used in the Network Device cPP for distributed TOEs. Such PPs are specifically reviewed and approved by NIAP. Once approved, the PP is included in Appendix A to this document. PPs that are not specifically constructed for use with a DSC cannot be approved, meaning that an ST cannot claim conformance to a "non-approved" PP and the DSC cPP and use Policy #28.

For evaluations performed according to Policy #28, an SFR can be associated with one or more TOE components—those TOE components can also implement the SFR in different ways and have different selections/assignments (if the SFR allows)—which aligns with how the responsibilities for the dependent technology and DSC for SFR implementation are allocated.

To support this model, the DSC ST identifies in its Supported Services Catalog the functions available to be leveraged by dependent technologies, based on the information in the DSC cPP SD. Each Approved Dependent Technology PP, in turn, specifies which requirements can be potentially satisfied by a DSC . If the satisfaction is partial or non-obvious, then there should also be some accompanying explanation so the Composed TOE ST writer and evaluators will be able to describe and evaluate the Composed TOE in an unambiguous manner.

In order to support exact conformance, each Approved Dependent Technology PP will "allow with" the DSC cPP, and vice versa. This entails each PP describing how it interacts with the other, which serves as the "placeholder" where the requirements in the dependent technology that are allowed to be satisfied by the DSC can be identified and described.

The Approved Dependent Technology PP will set the bounds on how a particular technology can use a DSC to satisfy certain SFRs. It is also allowed for the Composed TOE to not use an exported DSC service/interface at all, or may use a DSC service for one function but not use that same service for another function. This is reflected in the Composed TOE ST, where the ST author clearly identifies which requirements (or parts of requirements) are being satisfied by the DSC for specific functions described by the SFRs. The evaluator then applies the evaluation activities specified in the Approved Dependent Technology PP to the requirements that are not being satisfied by the DSC, and performs the appropriate activities (outlined in the next section) for those performed by the DSC. As with distributed TOEs, the evaluator will have to make sure that the SFR is completely and appropriately satisfied when looking at the dependent technology and DSC together, to ensure that there aren't gaps that are not addressed by either the dependent technology implementation or the DSC implementation.

Dependent Technology Evaluation Activities

The evaluation activities discussed in this section are those performed on the Composed TOE. These activities encompass activities related to the Approved Dependent Technology PP, the DSC cPP, the ST for the Composed TOE, design/interface, functional testing, and vulnerability analysis.

PP Evaluation Activities

The activities associated with the Approved Dependent Technology PPs and the DSC cPP (as described in this section) are different than other activities specified in this guidance in that they will need to be done only once for a particular dependent technology/DSC combination, rather than for every evaluation of a TOE against the combined PPs.

Two constructs may be used for a Composed TOE:

1) an ST that claims conformance to a PP-Configuration that contains that Approved Dependent Technology PP and the DSC cPP, or
2) an ST that claims conformance directly to both the Approved Dependent Technology PP and the DSC cPP.

The preferred method is to claim conformance to the PP-Configuration. Using a PP-Configuration gives structure to the evaluation of the combination, as well as provides a distinction between a product that uses a DSC and one that doesn't (because the one that doesn't would claim conformance only to the Approved Dependent Technology PP).

For either method, the technical work is the assessment of the identification of the requirements in the Approved Dependent Technology PP that can be satisfied by DSC functionality, and the scoping of those requirements. This work is not directly specified by any ACE or APE work unit, but is the same kind of activity as an "allowed with" determination for exact conformance—that is, it is dependent on the expertise of the technology experts, rather than a mechanical, editorial judgment. This activity is performed by the PP author groups, and is "completed" when each PP/cPP is added to the other's allowed-with list for exact conformance.

On the first evaluation of a unique combination of an Approved Dependent Technology PP and the DSC cPP, any issues with requirements specification, mismatches, etc. will be handled the same as with any other initial PP evaluation. If the combination is in a PP-Configuration, the evaluators will be expected to perform an ACE evaluation of the PP-Configuration according to the appropriate CEM work units.

Composed TOE ST Evaluation Activities

Evaluation of the Composed TOE ST is a key prerequisite to a successful evaluation of this type. This is because the Composed TOE ST maps Dependent Technology requirements to the DSC Supported Services Catalog, and is therefore the place where completeness and correctness of DSC use can be best assessed.

Information Required:

The Composed TOE ST must identify:

- Each SFR that is being fully or partially satisfied by the DSC (requirements section)

- The functionality being provided by the DSC (and by the dependent technology, for SFRs partially satisfied by the DSC) (TSS section)
- The interfaces invoked by the dependent technology (TSS section)

Evaluation Activity:

At the level of "ST evaluation," the evaluators must

- ensure that all functionality is completely addressed (if an SFR is being satisfied by both the DSC and the dependent technology);
- ensure the ST clearly identifies what the dependent technology is responsible for and what the DSC is responsible for;
- confirm that the SFRs that are being allocated to the DSC are allowed by the two PPs; and
- ensure that the interfaces identified by the ST are contained in the DSC Supported Services Catalog.[1]

Design/Interface Evaluation Activities

In general, the Approved Dependent Technology PPs do not require in-depth design information or analysis (no ADV_TDS, ADV_ARC, for example), and so such analysis is not required in the composed case. However, the evaluators will have to make sure that the dependent technology is using the interfaces exported by the DSC TOE in the way that they were evaluated by the DSC evaluation team. For example, if the DSC evaluation included only 256-bit AES-CBC in a crypto SFR and the dependent technology specified that it was using that crypto SFR (to be satisfied by the DSC product), but required 256-bit AES-GCM, then the evaluators should catch this type of mis-match even in the case where the DSC has implemented AES-GCM, but it does not appear in its Supported Services Catalog.

In cases such as this—where the DSC provides a function used by the dependent technology to satisfy an SFR, but that functionality wasn't evaluated in the DSC evaluation—the evaluators would just perform the evaluation activity listed in the Approved Dependent Technology PP for that SFR on the DSC-provided functionality. This is the same activity that would take place as for the case where the dependent technology implemented that functionality instead of the DSC, and so does not result in a meaningful loss of assurance in that functionality.

Information required:

- Interface descriptions in DSC evaluation report/ST (Supported Services Catalog),
- Interfaces used by dependent technology (in the Composed TOE ST TSS),
- calling sequence/context information to determine that used functionality was evaluated during DSC product evaluation (Supported Services Catalog).

Evaluation activity:

Assessment of interfaces to show that needs of the Composed TOE are met by evaluated DSC functionality.

[1] Note that the DSC Supported Services Catalog may appear in the DSC's ST or in a companion document that is logically part of the DSC's ST. The DSC's ST is distinct from the Composed TOE's ST, which is what is being referenced in these activities.

Functional Testing

One of the major "savings" in terms of evaluation effort in including an evaluated DSC in the Composed TOE evaluation is to reduce the testing effort. Requirements that are wholly met by DSC functionality do not have to be re-tested during the Composed TOE evaluation. But the DSC must be in its "evaluated configuration" when doing the Composed TOE test activities. Also, functions implemented by the dependent technology in response to SFRs in the Approved Dependent Technology PP that may have some reliance on functionality in the DSC are tested per the evaluation activities in the Approved Dependent Technology PP. For instance, if the dependent technology establishes TLS connections and uses the functions of the DSC to protect the credentials and roots of trust for the dependent technology used by the TLS functionality, the cryptographic primitives associated with this protection (which in this example are provided by the DSC) would not need to be re-tested, but the TLS functionality that uses these primitives *would* be tested in accordance to the TLS evaluation activities specified in the Approved Dependent Technology PP.

The testing of administrative interfaces also deserves some discussion. A DSC TOE may present interfaces that were exercised during the evaluation of the DSC TOE, but those interfaces may not be directly invoked by an administrator of a Composed TOE. The most common case will be for the dependent technology to present its own interface to the administrator, and then invoke the DSC interface (either directly, through a configuration setting, etc.). Therefore, the default case will be that the evaluators will be expected to completely test the interface presented by the Composed TOE, regardless of whether the underlying functionality is provided by the dependent technology or the DSC TOE.

Information required:

- SFRs that are met, either in whole or in part, by the DSC;
- test configuration (including specific DSC configuration)

Evaluation activity:

- Ensure DSC is included in test configuration;
- Ensure DSC is in its evaluated configuration;
- Test administrative interfaces as instructed by the Composed TOE's administrative guidance;
- Apart from administrative interface testing, do not repeat testing EAs for functionality implemented in response to SFRs allocated entirely to the DSC, or functionality that is wholly implemented by the DSC.

Vulnerability Analysis

The extent to which vulnerability analysis is performed (and the information that is required to perform it) is determined by the TC/iTC that produces a PP/cPP. For the DSC, the vulnerability information/analysis is current as of the evaluation of a particular DSC TOE, but additional information (vulnerabilities) may come to light after the evaluation is complete. The analysis performed by the Composed TOE evaluators should consider any deltas that may have emerged since the evaluation of the DSC component. This analysis should be to the same level of detail as was performed for the original DSC evaluation.

An obvious vulnerability scenario is the misuse (by the dependent technology) of a DSC interface that was not evaluated during the DSC evaluation that might impact the satisfaction of an SFR specified for the Composed TOE. While any vulnerabilities like this that are found should be addressed, it should not be required that the evaluators search for such vulnerabilities, because these vulnerabilities (vulnerabilities involving internal TOE interfaces) are typically not addressed in the specified dependent technology evaluation activities.

Information required:

- vulnerability sources (e.g., NVD) used in original DSC vulnerability analysis;
- terms used in the original DSC vulnerability analysis;
- information specified by DSC cPP to be provided to support vulnerability analysis;
- date of the DSC vulnerability analysis.

Evaluation activity:

The evaluators apply the same sources and terms used in the original vulnerability analysis, and address any new findings as part of the vulnerability analysis of the Composed TOE.

Other Considerations

Apart from the evaluation considerations mentioned above, two other areas are also affected by Policy #28: Assurance Maintenance and NIAP certificates for TOEs evaluated against an Approved Dependent Technology PP using a DSC.

Assurance Maintenance

Assurance Maintenance considerations are generally documented in NIAP Policy #17 and Publication #6. Since by its nature the dependent technology depends on the integrity of the DSCs, changes to the underlying DSC will affect the Composed TOE. For changes to the DSC that do not result in a re-evaluation (for instance, a vulnerability found in the DSC that requires an “emergency patch”), Policy #17 will apply not only to the DSC, but to all Composed TOEs that use that DSC.

Similarly, if the DSC undergoes a maintenance action, then Composed TOEs that use that DSC can also choose to undergo a maintenance action in order to remain up-to-date with the most current DSC. Procedures are performed in accordance with Publication #6. If a dependent technology does not choose to undergo a maintenance action, then the sunsetting of the certificate will apply according to the earliest evaluation date of either the DSC TOE or the Composed TOE.

Certificates

Policy #28 and this implementation guide allows significant flexibility between using Approved Dependent Technology PP-specified functionality and DSC cPP-specified functionality. Composed TOEs that make significant use of DSC functionality may have a different level of assurance in those functions than Composed TOEs that do not make use of a DSC. Therefore, certificates for Composed TOEs that meet an Approved Dependent Technology PP that also make use of DSC will have DSC information reflected on the certificate. Additionally, the VR for the TOE will contain a list of the services (and corresponding Approved Dependent Technology PP functions/SFRs) that are used from the list provided by the DSC, so that consumers will be able to determine the extent to which the DSC functionality is being used without having to read the details in the Security Target.

Appendix A : Approved Dependent Technology Protection Profiles

This appendix lists the Approved Dependent Technology PPs that are eligible for evaluation with a DSC TOE.

- *Watch this space!*