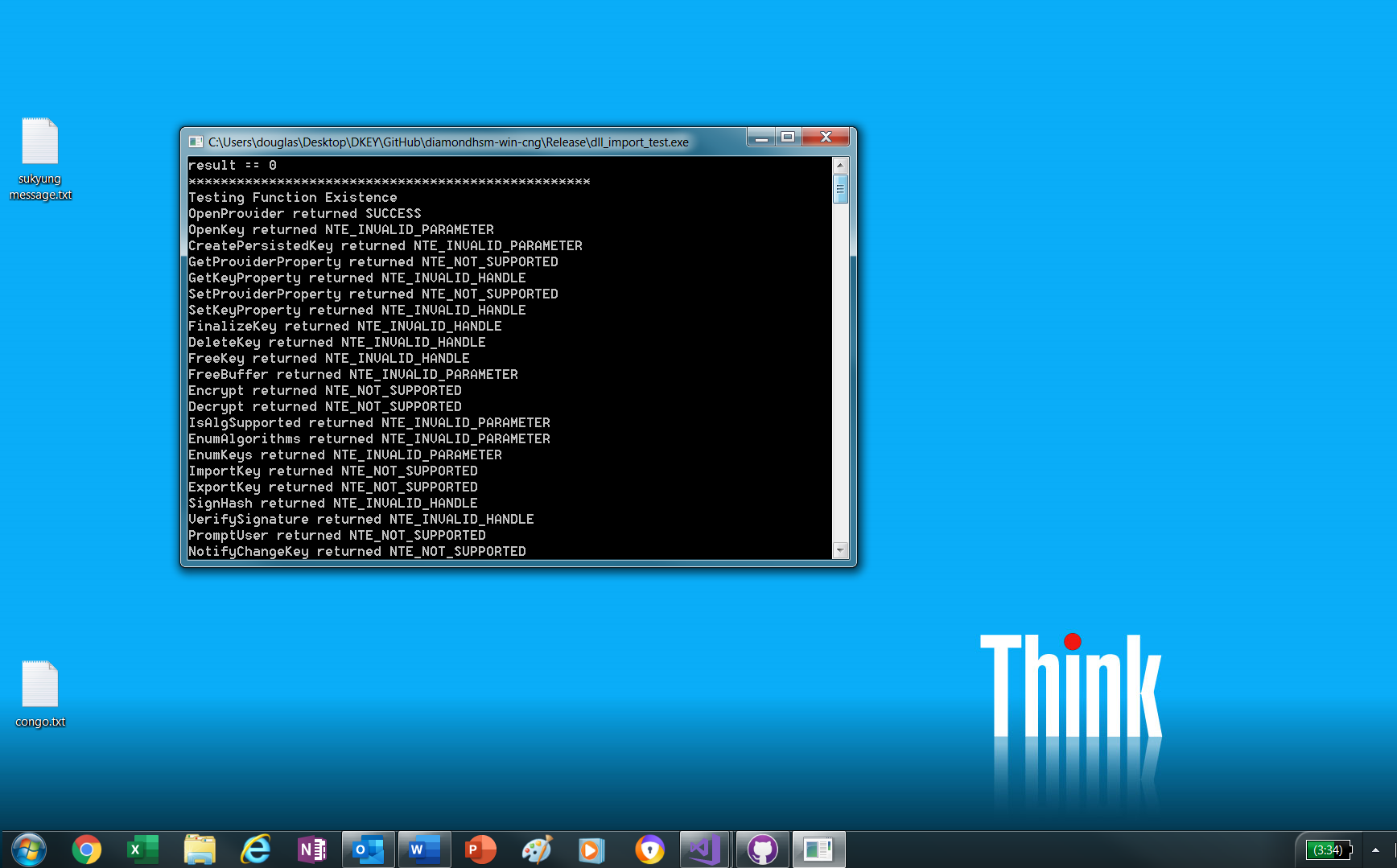
**Diamond-HSM Cryptography API: Next Gen Key Storage Provider**

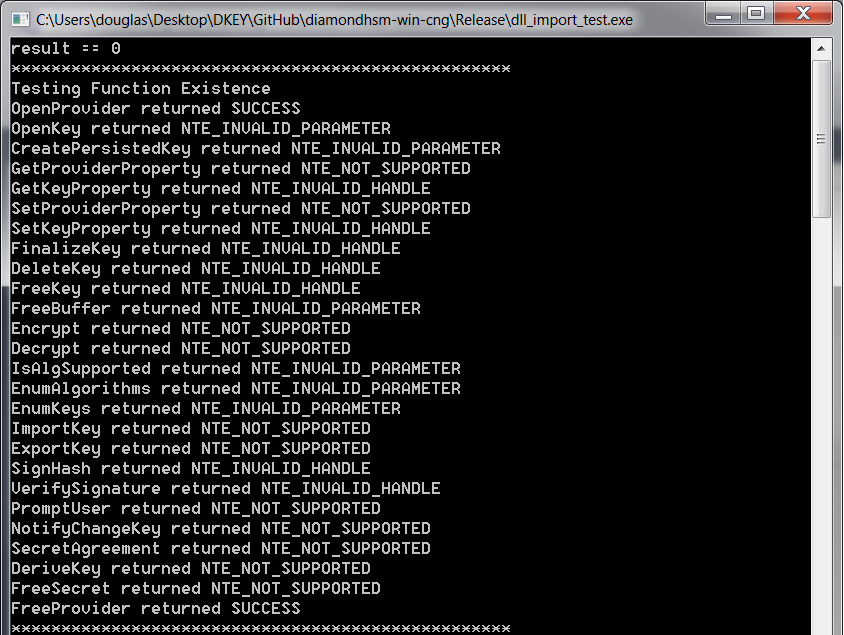
Test Results

The following document outlines the test from results from the “dll\_import\_test” project. This test is used to verify that the library operates properly on a Windows computer. That project performs unit test on the diamondhsm-cng-ksp\_Win32.dll and diamondhsm-cng-ksp\_x64.dll DLLs.



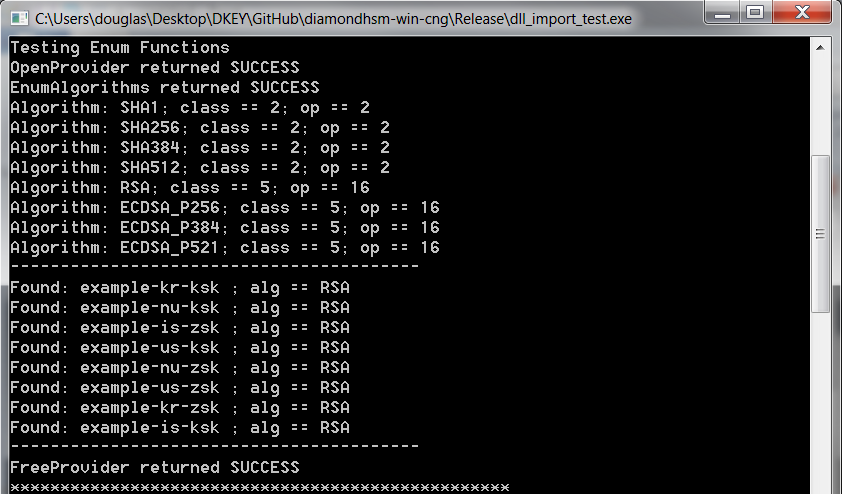
**Test 1.**

The first test tests all of the available CNG Key Storage Provider functions with incorrect parameters. This test is designed to fail. It checks that all of the functions can be exported. It also checks that parameter errors will not cause the DLL to crash.



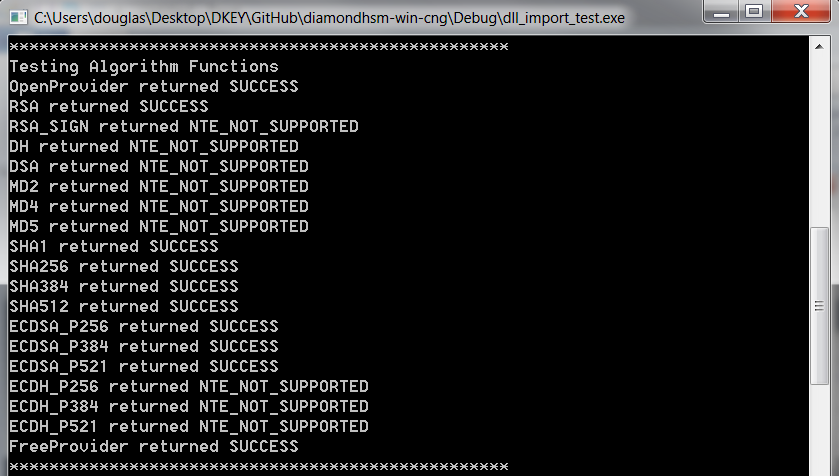
**Test 2**

The second test tests the enumeration functions inside of the KSP DLL. It first enumerates the hash and key types that the HSM supports. It then lists the keys that are currently on the HSM. In this test, the keys were first generated using a Linux computer using the BIND pkcs11-keygen tool.



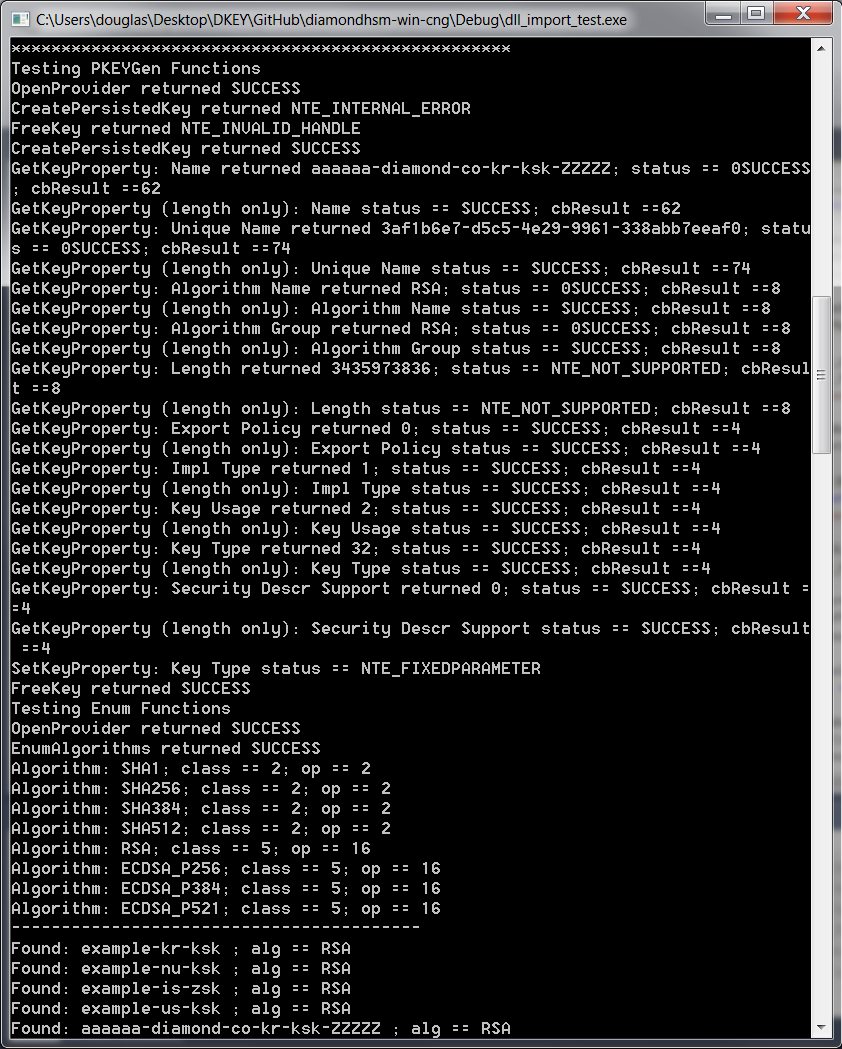
**Test 3**

Test 3 tests the IsAlgSupported function. It returns SUCCESS when used with an HSM supported algorithm.



**Test 4**

Test 4 generates a 1024-bit RSA key and then tests the GetKeyProperty function on the generated key.



**Test 5**

The final test tests ECDSA and RSA signing. It first generates new keys and then signs a SHA256 hash. It uses VerifySignature to verify the result. To confirm that VerifySignature is working, the resulting signature is changed and fed back into VerifySignature.

