AsicVault Performance Test Results

While during normal operation AsicVault hardware wallet performs 2 million rounds of PBKDF2 SHA-512, we have executed a sustainable performance test of 1 billion rounds. APP & SEC CPU utilization during the test shown is below 3%, background image rotation is performed entirely by the embedded GPU.

The results can be seen online at: https://vimeo.com/293211785

To capture the quickly changing results a little better using video camera we have used two alternating result sets. Currently active rows on the screen are surrounded by the vertical white lines.

Initial values of G, IDIG, ODIG, F and the pseudo-code to verify the test results is shown below:

```
unsigned long aulG[32]={
                0x8E1D9AF5, 0x3691E60D, 0xFF2FB92D, 0x5BB0FC85, 0x8C705541, 0x9B9882A2, 0x0FCB2CFB, 0x62FA32CB,
                0x6E9A2F8C, 0xB7F2B7CF, 0x373BE4F3, 0xBD41A907, 0xAC8D4186, 0x07838F05, 0xFB1802B5, 0xB03BF58F,
                0x80000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000,
                0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000600  };
unsigned long aulIDIG[16]={
                0x046A1CE4, 0x3EC332DE, 0xDCC6760B, 0xC7CAC840, 0x9A1F8365, 0x4F888B9F, 0x7669F084, 0x9F2DD14D,
                0x19CA4BA7, 0x3F185589, 0x854BF579, 0x737BEDF0, 0x9C32AD50, 0x0B6854C5, 0xA812F42A, 0xCE19AAAD  };
unsigned long aulODIG[16]={
                0x8AF833DD, 0x3B2FABC3, 0x3C9C5EBD, 0x339246CD, 0xD1D9F5C3, 0x9E5E2FED, 0x2D0CBC5E, 0xCD246334,
                0xBA822636, 0x7151EA2E, 0x7892D4D9, 0x8CC519EA, 0x17188931, 0xEE47164D, 0xB250736D, 0x98D81B9A  };
unsigned long aulF[16]={
                0x8E1D9AF5, 0x3691E60D, 0xFF2FB92D, 0x5BB0FC85, 0x8C705541, 0x9B9882A2, 0x0FCB2CFB, 0x62FA32CB,
                0x6E9A2F8C, 0xB7F2B7CF, 0x373BE4F3, 0xBD41A907, 0xAC8D4186, 0x07838F05, 0xFB1802B5, 0xB03BF58F  };

void test_sha512_speed( void )
        {
        PBKDF2_HMAC_SHA512_CTX pctx;
        for( int i=0; i<32; i+=2 )
                {
                ((unsigned long*)pctx.g)[i]=aulG[i+1];
                ((unsigned long*)pctx.g)[i+1]=aulG[i];
                }
        for( int i=0; i<16; i+=2 )
                {
                ((unsigned long*)pctx.idig)[i]=aulIDIG[i+1];
                ((unsigned long*)pctx.idig)[i+1]=aulIDIG[i];
                }
        for( int i=0; i<16; i+=2 )
                {
                ((unsigned long*)pctx.odig)[i]=aulODIG[i+1];
                ((unsigned long*)pctx.odig)[i+1]=aulODIG[i];
                }
        for( int i=0; i<16; i+=2 )
                {
                ((unsigned long*)pctx.f)[i]=aulF[i+1];
                ((unsigned long*)pctx.f)[i+1]=aulF[i];
                }
        pctx.first = 0;
        for( int i=0; i<1000000000; )
                {
                i+=10000;
                printf( "%10u: ", i );
                pbkdf2_hmac_sha512_Update( &pctx, 10000 );
                }
        }
```

These test results can be also used to calculate the time that AsicVault hardware wallet needs to perform 2 million rounds of PBKDF2 SHA-512 and it can be directly compared to other wallets to verify the performance difference claims.