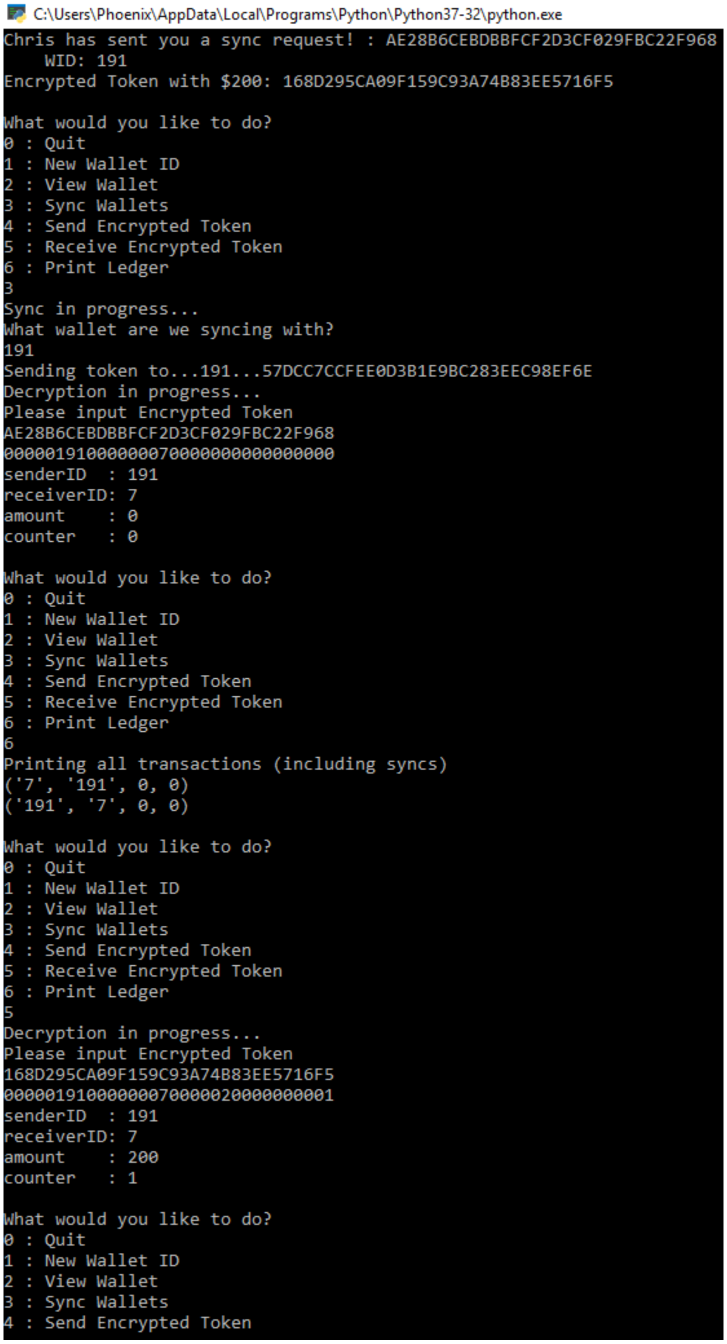
User Input   Notifications   Smart Wallet – Sample Output   Jeffrey Murray

```
Chris has sent you a sync request :
AE28B6CEBDBBFCF2D3CF029FBC22F968
   WID: 191
Encrypted Token with $200:
168D295CA09F159C93A74B83EE5716F5

2 : View Wallet
---StartOFWallet---
Balance: $0
       SID: 1876007
kWallet:
90F284DFCA791EFDF52EC5837C7200374B9F09
EE42E80D37473D8654526C16B5
You must sync your wallet!
----EndOfWallet----

3 : Sync Wallets
Sync in progress...
What wallet are we syncing with?
191
Sending token to...191...
57DCC7CCFEE0D3B1E9BC283EEC98EF6E
Decryption in progress...
Please input Encrypted Token
AE28B6CEBDBBFCF2D3CF029FBC22F968
00000191000000007000000000000000
senderID  : 191
receiverID: 7
amount    : 0
counter   : 0

5 : Receive Encrypted Token
Decryption in progress...
Please input Encrypted Token
168D295CA09F159C93A74B83EE5716F5
00000191000000007000002000000001
senderID  : 191
receiverID: 7
amount    : 200
counter   : 1
```

```
2 : View Wallet
---StartOFWallet---
Balance: $200
       SID: 1876007
 kWallet:
90F284DFCA791EFDF52EC5837C7200374B9F09
EE42E80D37473D8654526C16B5
Synced Wallet: 191
Current Count: 2
----EndOfWallet----
6 : Print Ledger
Printing all transactions (including syncs)
('7', '191', 0, 0)
('191', '7', 0, 0)
('191', '7', 200, 1)

4 : Send Encrypted Token
Amount to send? :
200
Updated Balance: $0
Encrypted token:
9120B9B5B9CD91BC42CEC9B8ADCDDA3B

6 : Print Ledger
Printing all transactions (including syncs)
('7', '191', 0, 0)
('191', '7', 0, 0)
('191', '7', 200, 1)
('7', '191', 200, 2)

0 : Quit
Thank you for using Smart Wallet
by Jeffrey Murray
```

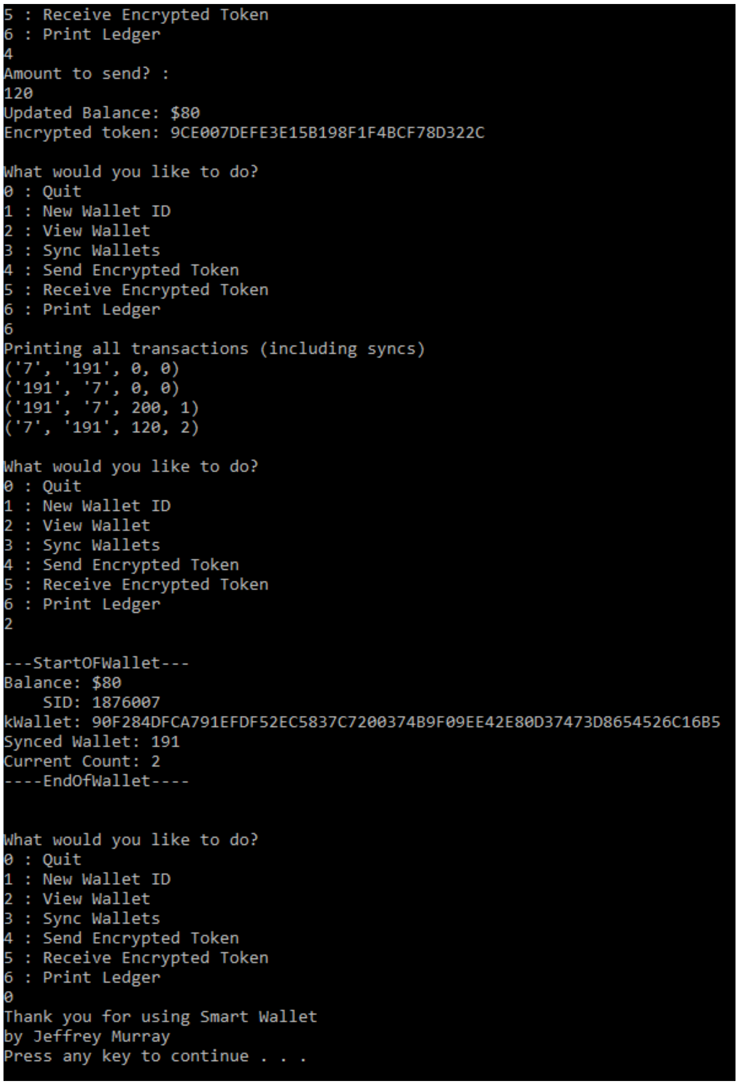
User Input Notifications Smart Wallet – Sample Output Jeffrey Murray



C:\Users\Phoenix\AppData\Local\Programs\Python\Python37-32\python.exe

```
Chris has sent you a sync request! : AE28B6CEBDBBFCF2D3CF029FBC22F968
    WID: 191
Encrypted Token with $200: 168D295CA09F159C93A74B83EE5716F5

What would you like to do?
0 : Quit
1 : New Wallet ID
2 : View Wallet
3 : Sync Wallets
4 : Send Encrypted Token
5 : Receive Encrypted Token
6 : Print Ledger
3
Sync in progress...
What wallet are we syncing with?
191
Sending token to...191...57DCC7CCFEE0D3B1E9BC283EEC98EF6E
Decryption in progress...
Please input Encrypted Token
AE28B6CEBDBBFCF2D3CF029FBC22F968
00000191000000070000000000000000
senderID  : 191
receiverID: 7
amount    : 0
counter   : 0

What would you like to do?
0 : Quit
1 : New Wallet ID
2 : View Wallet
3 : Sync Wallets
4 : Send Encrypted Token
5 : Receive Encrypted Token
6 : Print Ledger
6
Printing all transactions (including syncs)
('7', '191', 0, 0)
('191', '7', 0, 0)

What would you like to do?
0 : Quit
1 : New Wallet ID
2 : View Wallet
3 : Sync Wallets
4 : Send Encrypted Token
5 : Receive Encrypted Token
6 : Print Ledger
5
Decryption in progress...
Please input Encrypted Token
168D295CA09F159C93A74B83EE5716F5
00000191000000070000020000000001
senderID  : 191
receiverID: 7
amount    : 200
counter   : 1

What would you like to do?
0 : Quit
1 : New Wallet ID
2 : View Wallet
3 : Sync Wallets
4 : Send Encrypted Token
```

Picture proof working console. This is a demo where Chris has sent me a request to sync wallets AE28B6CEBDBBFCF2D3CF029FBC22F968
And a token with $200!
168D295CA09F159C93A74B83EE5716F5

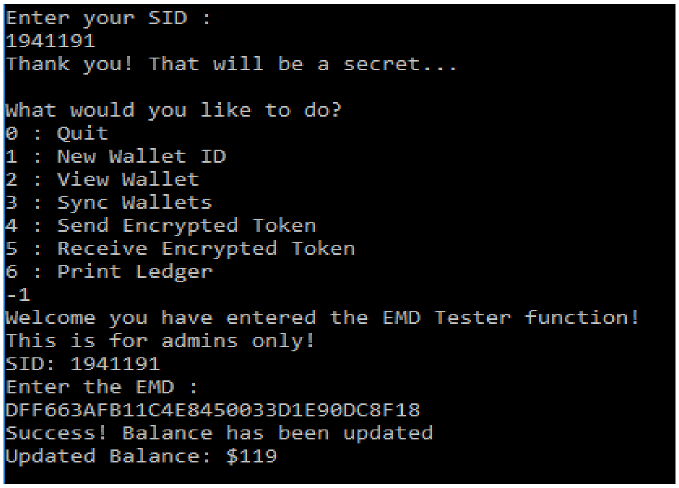


```
5 : Receive Encrypted Token
6 : Print Ledger
4
Amount to send? :
120
Updated Balance: $80
Encrypted token: 9CE007DEFE3E15B198F1F4BCF78D322C

What would you like to do?
0 : Quit
1 : New Wallet ID
2 : View Wallet
3 : Sync Wallets
4 : Send Encrypted Token
5 : Receive Encrypted Token
6 : Print Ledger
6
Printing all transactions (including syncs)
('7', '191', 0, 0)
('191', '7', 0, 0)
('191', '7', 200, 1)
('7', '191', 120, 2)

What would you like to do?
0 : Quit
1 : New Wallet ID
2 : View Wallet
3 : Sync Wallets
4 : Send Encrypted Token
5 : Receive Encrypted Token
6 : Print Ledger
2

---StartOFWallet---
Balance: $80
    SID: 1876007
kWallet: 90F284DFCA791EFDF52EC5837C7200374B9F09EE42E80D37473D8654526C16B5
Synced Wallet: 191
Current Count: 2
----EndOfWallet----


What would you like to do?
0 : Quit
1 : New Wallet ID
2 : View Wallet
3 : Sync Wallets
4 : Send Encrypted Token
5 : Receive Encrypted Token
6 : Print Ledger
0
Thank you for using Smart Wallet
by Jeffrey Murray
Press any key to continue . . .
```

2 Vulnerabilities with this application

First, Relay attacks can be used to send sync wallet requests. This would be corrected by comparing the counter to the main_counter in the program, for any counter == m_count increments ++m_count. The new tokens counter > m_count to accept them as valid tokens.

Second, there is an admin function available “-1” into console page that can allow any encrypted EMD with the current SID to input money Ex. I input Chris’s SID in, input token given to us on canvas, $119 is added to my account. No sync, token, or any secure transmission required.



```
Enter your SID :
1941191
Thank you! That will be a secret...

What would you like to do?
0 : Quit
1 : New Wallet ID
2 : View Wallet
3 : Sync Wallets
4 : Send Encrypted Token
5 : Receive Encrypted Token
6 : Print Ledger
-1
Welcome you have entered the EMD Tester function!
This is for admins only!
SID: 1941191
Enter the EMD :
DFF663AFB11C4E8450033D1E90DC8F18
Success! Balance has been updated
Updated Balance: $119
```

Third, another security issue is that there is no login or verification to prove that you are Chris or SID 1941191. I can become Tim SID: 1941193. With easy I can accept tokens as these users just by knowing their SID. This would be very problematic in the real world. Optionally creating a UW net ID login that would fetch their credentials from UW would be satisfactory authentication.

Final Test ** PASSED ** Using two windows of my program to pass tokens back and forth to test how my program handles two wallets real time encryption and decryption.