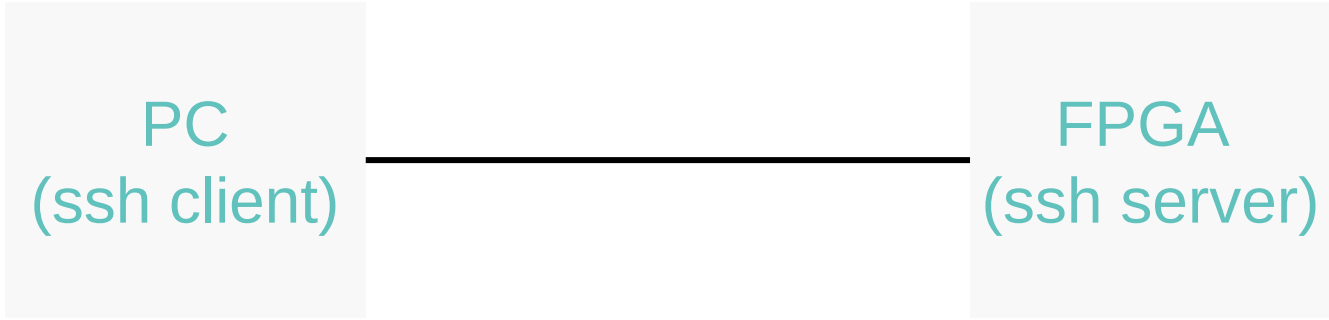
PUFsecurity Utility User Guide.

2022 October

PUFsecurity
AN eMemory COMPANY

Architecture and Scripts



- **Two scripts are provided for RNG get_info and get_random APIs**
  - get_info_xxx.sh :
    - generates a JSON format file "get_info.txt" with device id and public key.
  - get_random_xxx.sh :
    - generates a JSON format file "get_random.txt" with 8 bytes random number and its signature

	Client Script	Server Script
Get RNG info	get_info_client.sh	get_info_server.sh
Get Random	get_random_client.sh	get_random_server.sh

File Location in the FPGA.

- **Utility and script file location in the FPGA**
  - **/home/root/projects/pufs_util**

```
root@pufiot:~/projects/pufs_util# ls -al
total 244
drwxr-xr-x    2 root     root          4096 Oct 26 08:40 .
drwxr-xr-x    4 root     root          4096 Oct 26 04:19 ..
-rw-r--r--    1 root     root           360 Oct 26 08:36 client_script_example.tgz
-rwxr-xr-x    1 root     root           165 Oct 26 04:19 get_info_server.sh
-rwxr-xr-x    1 root     root           270 Oct 26 04:19 get_random_server.sh
-rwxr-xr-x    1 root     root        227036 Oct 26 04:30 pufs_utility
```

File Name	Description
client_script_example.tgz	Example client scripts executed on the ssh client machine. (There are 2 files in the tarball: get_info_client.sh and get_random_client.sh)
get_info_server.sh	Bash script to get device id and public key.
get_random_server.sh	Bash script to get 8 bytes random number and its signature.
pufs_utility	PUFsecurity utility execution file

Configuration Setting in Example Client Scripts

- **FPGA IP and SSH port settings in the example client scripts**
  - IP_ADDR="172.16.1.91"
  - PORT="22238“

  - Customer should modify the IP_ADDR and PORT number based on your environment.
  - The default port for SSH client connections is 22.

Get RNG Information (on FPGA)

- **Command**
  - get_info_server.sh
- **Script location**
  - /home/root/projects/pufs_util
- **Execution Example:**
  - Command:

```
cd /home/root/projects/pufs_util
./get_info_server.sh
```

  - Output
    - “get_info.txt”


```
{"uid":"puf_000a35001e56_e62d6f2b13038f52cf99fd4d492b2a4f7932984fc4491de4eca5eefb
81187b08","public_key":"af92bad2f20cb54bf1212d7596ad5d795e4748d3ead0696bf21a02dd
6352d3c12d8d09840123b81000b3d512e97d39fd9a24f200c7a062c37d93f09a2ee3fd4a"}
```

Get Random Number (on FPGA)

- **Command**
  - get_random_server.sh
- **Script location**
  - /home/root/projects/pufs_util
- **Execution Example:**
  - Command:

```
cd /home/root/projects/pufs_util
./get_random_server.sh
```

  - Output
    - “get_random.txt”

```
{"rn":"3108b4adf0757b25","signature_payload":"bfa8769e4144af056856f286b6783ca46e257
209b64755758ba10c88fae06bf702c84e63fdfd70fc56b2c3fe08a19acddd7e677251df825597
dc151597499a50"}
```


Classified as Confidential

Get RNG info or RN from the Remote PC

- **Environment setting**
  - Modify IP and port settings in get_info_client.sh and get_random_client.sh

- **Get Info**
  - Command:

```
./get_info_client.sh
```

  - Result
    - File “get_info.txt” is generated in the same place where the command is executed.

- **Get Info**
  - Command:

```
./get_random_client.sh
```

  - Result
    - File “get_random.txt” is generated in the same place where the command is executed.