

New York University Tandon School of Engineering

CS-GY 9223: Software Supply Chain Security

Assignment 1 | Sanchit Sahay | ss19723

Cosign:

```
$ > cosign sign-blob artifact.md --bundle artifact.bundle
[...]
The sigstore service, hosted by sigstore a Series of LF Projects, LLC, is provided pursuant to the Hosted Project Tools Term
s of Use, available at https://lfprojects.org/policies/hosted-project-tools-terms-of-use/.
Note that if your submission includes personal data associated with this signed artifact, it will be part of an immutable re
cord.
This may include the email address associated with the account with which you authenticate your contractual Agreement.
This information will be used for signing this artifact and will be stored in public transparency logs and cannot be removed
later, and is subject to the Immutable Record notice at https://lfprojects.org/policies/hosted-project-tools-immutable-records/.

By typing 'y', you attest that (1) you are not submitting the personal data of any other person; and (2) you understand and agree to
the statement and the Agreement terms at the URLs listed above.
Are you sure you would like to continue? [y/N] y
Generating ephemeral keys...
Your browser will now be opened to:
https://oauth2.sigstore.dev/auth?access_type=online&client_id=sigstore&code_challenge=0Eu6cenovFcs_03vzIpC40Ib2J3cwyUdElPIfU_ba
fE&code_challenge_method=S256&nonce=32weyoCJtdylzqNoKswtqlsvEd&redirect_uri=http%3A%2F%2Flocalhost%3A56528%2Fauth%2Fcallback&respon
se_type=code&scope=openid+email+state=32weylZuiHYrpgDRHdLlkYWkMB
Retrieving signed certificate...
Successfully verified SCT...
Using payload from: artifact.md
tlog entry created with index: 540288699
Wrote bundle to file artifact.bundle
MEUCIQCsB2yLkQMVAw2RStUAPu/vU46AVGgBPYFI6pLpndmzlAIgaEujETghOWoQzp05e2Daeyv8Gx50Kuj6x+2blqXgVRg=
$ > 
```

Latest Checkpoint:

```
(amlds) $ > python3 main.py -c
{
    "inactiveShards": [
        {
            "rootHash": "4d006aa46efcb607dd51d900b1213754c50cc9251c3405c6c2561d9d6a2f3239",
            "signedTreeHead": "rekor.sigstore.dev - 3904496407287907110\nn4163431\nnTQBqpG78tgfd
UdkAsSE3VMMySUcNAXGwlYdnWovMjk=\n\n\u2014 rekor.sigstore.dev wNI9ajBFAiBUM9om2kVJemZEJmLW296q
UxDLdw8GjqF2YMeiqmpUMgIhAOsXr4/cjQ/i7rNyy09i8sYMWp715URVQhbJh10LYlRW\n",
            "treeID": "3904496407287907110",
            "treeSize": 4163431
        },
        {
            "rootHash": "2b9c578071e120aa84c9858783daa671565e4165f3a7dfa199aad81940299d8e",
            "signedTreeHead": "rekor.sigstore.dev - 2605736670972794746\nn117740831\nnK5xXgHHhIK
qEyYWHg9qmcVZeQWXzp9+hmarYGUApnY4=\n\n\u2014 rekor.sigstore.dev wNI9ajBFAiEaxzV2NYqoig4cLtUohi
dFiUw2nyMJXI+XxhvqUcHSlooCIEB3puNAhKwBleGWE4ybpmPT6Z2s5JK0/LtmswZINNrcF\n",
            "treeID": "2605736670972794746",
            "treeSize": 117740831
        }
    ],
    "rootHash": "73048341619c7a3e73861d590d6bd7922c536cd2ddc7767db2629dd4e2d40cd1",
    "signedTreeHead": "rekor.sigstore.dev - 1193050959916656506\nn418435196\nncwSDQWGcej5zhh1ZDW
vXkixTbNLdx3Z9smKd10LUDNE=\n\n\u2014 rekor.sigstore.dev wNI9ajBEAiB/e30+lYaT/E61PG6L8uubKRRNMm
MWAhEgpzbHMTNfgwIgYce4vhF2Rwh0kBtlQ9ourwcN6Z8F33gQ70ZihPcTa4I=\n",
    "treeID": "1193050959916656506",
    "treeSize": 418435196
}
(amlds) $ > 
```

```
[1] 2:zsh* 3:zsh 4:docker 5:docker- 6:docker      "10-20-2-188.dynapool." 01:05 20-Sep-25
```

Inclusion Verification, Consistency Verification:

```
(amlds) $ > python3 main.py --inclusion 540283374 --artifact artifact.md
Offline verification successful
(amlds) $ > python3 main.py --consistency --tree-id 1193050959916656506 --tree-size 418434214
--root-hash 5f884c9698981d5a8d35bde3954843aa2d0a5290ec09f5b7d2eebc3373b33ef9
Consistency verification successful
(amlds) $ > 
```