

Sti-shaken log extraction



Purpose

- Push sti-verify log from local file to remote servers
- Remote server check if the log/errir is now for “today” and if so:
 - Send email
 - Send to mattermost via restful
 - Insert email event to DB
- Insert received log to postgres
- Provide public API for user to stop receiving email

What we need

- Two node.js program.
 - One running on servers where logs are produced
 - One running on central server as a daemon process using systemctl status/start/stop

Client side

Client to do

- Client should scan the log and find new log to send to backend.
- Client program should log new log identification and sending to backend event to log file

Daily Verify_error log files

```
-rw-r--r--. 1 root root 1/122483 Mar 22 09:12 2025_03_22_shaken_verif_error.log
[root@64-185-235-194 verif_err]# wc *
11203843 68198576 1185933110 2025_02_26_shaken_verif_error.log
5519185 34768252 600916182 2025_02_27_shaken_verif_error.log
5536237 34981078 602896253 2025_02_28_shaken_verif_error.log
589501 3858036 66036185 2025_03_01_shaken_verif_error.log
141591 942458 15776333 2025_03_02_shaken_verif_error.log
6368460 40888576 710050462 2025_03_03_shaken_verif_error.log
9893626 63310705 1101996932 2025_03_04_shaken_verif_error.log
15094719 94849018 1677474440 2025_03_05_shaken_verif_error.log
11388801 73626048 1276975407 2025_03_06_shaken_verif_error.log
17073426 112710603 1966217235 2025_03_07_shaken_verif_error.log
2158221 14180648 245175852 2025_03_08_shaken_verif_error.log
377773 2437179 40743084 2025_03_09_shaken_verif_error.log
21591958 145049583 2535234102 2025_03_10_shaken_verif_error.log
22328179 149795156 2615603251 2025_03_11_shaken_verif_error.log
24099514 161322952 2830792868 2025_03_12_shaken_verif_error.log
18198368 121794318 2135360692 2025_03_13_shaken_verif_error.log
15426344 103394083 1808474608 2025_03_14_shaken_verif_error.log
2507383 16585201 291818014 2025_03_15_shaken_verif_error.log
299736 1941948 33353588 2025_03_16_shaken_verif_error.log
17109738 114334122 2002894448 2025_03_17_shaken_verif_error.log
20720499 136554310 2393860226 2025_03_18_shaken_verif_error.log
23067169 152293485 2683549049 2025_03_19_shaken_verif_error.log
24045593 156182344 2767704771 2025_03_20_shaken_verif_error.log
21291673 137623282 2451323318 2025_03_21_shaken_verif_error.log
159547 1012124 17135858 2025_03_22_shaken_verif_error.log
296191084 1942634085 34057296268 total
[root@64-185-235-194 verif_err]# pwd
/opt/denovo_v6/dnl_softswitch/shaken_log/verif_err
[root@64-185-235-194 verif_err]#
```

```
root@64-185-235-194 verif_err]# head -100 2025_03_22_shaken_verif_error.log [more]
=====
2025-03-22 00:00:00 Identity: 'eyJhbGciOiJIUzI1NiIsInR5cCI6ImlrInNoYmVtbiIjOnRoRCw6LWl5ZjZkcy50ZWxvbm1lbS5UZXQvcmc9dC1HMSS5jcnc0fQ.eyJhdHRlc3Q3O1JDIIiwZGVzdCIey3B0iEwYixNzg3NzY4MDIzMyJdfSwiaWF0IjoXNzQyNjAxNjAyLCJ3cmVmlnIjpwInRuIjoIMTYMeMzIxODAxZWZib3p2Z2lkIjoImzMGMGM0ZWtmNQ0Yy08NDFlTHYmYmUzNGM0NzQ0OTUvTkViLn8.ievv6LoSe4oBatYX9Kz5CBcAQnwZgmw6kYxyZCyk2cmPAKMyleKRQINORq3Wk83sieY_jtQjPMMyCvjz_1g;info=https://certs.telonium.net/root-G1.crt;alg=ES256;ppt=shaken'
Error stack (top to bottom, outermost first - deepest last):
[ERR 0] libstirshaken/src/stir_shaken_verify.c:542: [error_code: 193] JWT failed verification with X509 cert path check
[ERR 1] libstirshaken/src/stir_shaken_verify.c:458: [error_code: 180] JWT did not pass verification
[ERR 2] libstirshaken/src/stir_shaken_verify.c:407: [error_code: 190] JWT did not pass signature check
[libstirshaken git version: ]

=====
2025-03-22 00:00:00 Identity: 'eyJhbGciOiJIUzI1NiIsInR5cCI6ImlrInNoYmVtbiIjOnRoRCw6LWl5ZjZkcy50ZWxvbm1lbS5UZXQvcmc9dC1HMSS5jcnc0fQ.eyJhdHRlc3Q3O1JDIIiwZGVzdCIey3B0iEwYixNzg3NzY4MDIzMyJdfSwiaWF0IjoXNzQyNjAxNjAyLCJ3cmVmlnIjpwInRuIjoIMTYMeMzIxODAxZWZib3p2Z2lkIjoImzMGMGM0ZWtmNQ0Yy08NDFlTHYmYmUzNGM0NzQ0OTUvTkViLn8.ievv6LoSe4oBatYX9Kz5CBcAQnwZgmw6kYxyZCyk2cmPAKMyleKRQINORq3Wk83sieY_jtQjPMMyCvjz_1g;info=https://certs.telonium.net/root-G1.crt;alg=ES256;ppt=shaken'
Error stack (top to bottom, outermost first - deepest last):
[ERR 0] libstirshaken/src/stir_shaken_verify.c:542: [error_code: 193] JWT failed verification with X509 cert path check
[ERR 1] libstirshaken/src/stir_shaken_verify.c:458: [error_code: 180] JWT did not pass verification
[ERR 2] libstirshaken/src/stir_shaken_verify.c:407: [error_code: 190] JWT did not pass signature check
[libstirshaken git version: ]

=====
2025-03-22 00:00:00 Identity: 'eyJhbGciOiJIUzI1NiIsInR5cCI6ImlrInNoYmVtbiIjOnRoRCw6LWl5ZjZkcy50ZWxvbm1lbS5UZXQvcmc9dC1HMSS5jcnc0fQ.eyJhdHRlc3Q3O1JDIIiwZGVzdCIey3B0iEwYixNzg3NzY4MDIzMyJdfSwiaWF0IjoXNzQyNjAxNjAyLCJ3cmVmlnIjpwInRuIjoIMTYMeMzIxODAxZWZib3p2Z2lkIjoImzMGMGM0ZWtmNQ0Yy08NDFlTHYmYmUzNGM0NzQ0OTUvTkViLn8.ievv6LoSe4oBatYX9Kz5CBcAQnwZgmw6kYxyZCyk2cmPAKMyleKRQINORq3Wk83sieY_jtQjPMMyCvjz_1g;info=https://certs.telonium.net/root-G1.crt;alg=ES256;ppt=shaken'
Error stack (top to bottom, outermost first - deepest last):
[ERR 0] libstirshaken/src/stir_shaken_verify.c:542: [error_code: 193] JWT failed verification with X509 cert path check
[ERR 1] libstirshaken/src/stir_shaken_verify.c:458: [error_code: 180] JWT did not pass verification
[ERR 2] libstirshaken/src/stir_shaken_verify.c:407: [error_code: 190] JWT did not pass signature check
[libstirshaken git version: ]

=====
2025-03-22 00:00:00 Identity: 'eyJhbGciOiJIUzI1NiIsInR5cCI6ImlrInNoYmVtbiIjOnRoRCw6LWl5ZjZkcy50ZWxvbm1lbS5UZXQvcmc9dC1HMSS5jcnc0fQ.eyJhdHRlc3Q3O1JDIIiwZGVzdCIey3B0iEwYixNzg3NzY4MDIzMyJdfSwiaWF0IjoXNzQyNjAxNjAyLCJ3cmVmlnIjpwInRuIjoIMTYMeMzIxODAxZWZib3p2Z2lkIjoImzMGMGM0ZWtmNQ0Yy08NDFlTHYmYmUzNGM0NzQ0OTUvTkViLn8.ievv6LoSe4oBatYX9Kz5CBcAQnwZgmw6kYxyZCyk2cmPAKMyleKRQINORq3Wk83sieY_jtQjPMMyCvjz_1g;info=https://certs.telonium.net/root-G1.crt;alg=ES256;ppt=shaken'
Error stack (top to bottom, outermost first - deepest last):
[ERR 0] libstirshaken/src/stir_shaken_verify.c:542: [error_code: 193] JWT failed verification with X509 cert path check
[ERR 1] libstirshaken/src/stir_shaken_verify.c:458: [error_code: 180] JWT did not pass verification
[ERR 2] libstirshaken/src/stir_shaken_verify.c:407: [error_code: 190] JWT did not pass signature check
[libstirshaken git version: ]

=====
2025-03-22 00:00:00 Identity: 'eyJhbGciOiJIUzI1NiIsInR5cCI6ImlrInNoYmVtbiIjOnRoRCw6LWl5ZjZkcy50ZWxvbm1lbS5UZXQvcmc9dC1HMSS5jcnc0fQ.eyJhdHRlc3Q3O1JDIIiwZGVzdCIey3B0iEwYixNzg3NzY4MDIzMyJdfSwiaWF0IjoXNzQyNjAxNjAyLCJ3cmVmlnIjpwInRuIjoIMTYMeMzIxODAxZWZib3p2Z2lkIjoImzMGMGM0ZWtmNQ0Yy08NDFlTHYmYmUzNGM0NzQ0OTUvTkViLn8.ievv6LoSe4oBatYX9Kz5CBcAQnwZgmw6kYxyZCyk2cmPAKMyleKRQINORq3Wk83sieY_jtQjPMMyCvjz_1g;info=https://certs.telonium.net/root-G1.crt;alg=ES256;ppt=shaken'
Error stack (top to bottom, outermost first - deepest last):
[ERR 0] libstirshaken/src/stir_shaken_verify.c:542: [error_code: 193] JWT failed verification with X509 cert path check
[ERR 1] libstirshaken/src/stir_shaken_verify.c:458: [error_code: 180] JWT did not pass verification
[ERR 2] libstirshaken/src/stir_shaken_verify.c:407: [error_code: 190] JWT did not pass signature check
[libstirshaken git version: ]
```

- We need to push these to backen in json format
- {
 { identity: ... }, {err0: ...}, {err1:...}, {err2:...}
}

Server side

Remote server

- Push Log to DB
- Check if the certificate is NEW for today
- If New, then email out
- If New, log to mattermost
- If New, log to log file.

Speed

- The server side, receive the request, should immediately push to DB.
- The server side should not hold the request. It should return a uuid and do the task at an asynchronous way.
- The client should not need to wait for server to do the task.

Table: STI-error

Field Name	Type	Description
uuid	uuid	This is auto generated key
identity_header	varchar	
err1		
err2		
err3		
from_ip	ipv4	This is client_ip that server to server.
cert_url	varchar	Url in the identity header. Ex: https://cr.sansay.com/306K/429C7C70711E3820F0B8E1DEAE6FF3262264BFD0.pem
certificate	varchar	Cert download from cert_url

Table: STI-error

Field Name	Type	Description
clear_text_cert	varchar	
signature	varchar	Decryption of the identity header
ani	varchar	
dnis	varchar	
CA	varchar	
not_after	timestamp	
not_before	timestamp	
OCN	varchar	
Origination	varchar	
Country	varchar	

Table: STI-error

Field Name	Type	Description
Identity_error	varchar	
cert_url_found	Boolean	The cert_url is able to download cert or not.
is_repeated	boolean	If the cert_url's content is same as one of the error in previous records of today, then it is true, else it is false. We need this because we only want to send error once.

```
[root@ns508297 tmp]# curl https://cr.sansay.com/306K/429C7C70711E3820F0B8E1DEAE6FF3262264BFD0.pem
```

```
[root@ns508297 tmp]# curl https://cr.sansay.com/306K/429C7C70711E3820F0B8E1DEAE6FF3262264E
```

END OF CERTIFICATE

Get Clear Text of the Cert (clear_text_certificate)

```
[[root@ns508297 tmp]# curl https://cr.sansay.com/306K/429C7C70711E3820F08B8E1DEAE6FF3262264BFD0.pem > /tmp/certificate.txt
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left     Speed

100 2031 100 2031    0     0  3732      0 --:--:-- --:--:-- --:--:-- 3733
[root@ns508297 tmp]#
[root@ns508297 tmp]#
[root@ns508297 tmp]# openssl x509 -text -noout -in /tmp/certificate.txt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            42:9c:7c:70:71:1e:38:20:f0:b8:e1:de:ae:6f:f3:26:22:64:bf:d0
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=US, ST=California, O=Sansay Corporation, OU=Sansay CA, CN=SHAKEN Sansay Intermediate CA US WEST 1
        Validity
            Not Before: Feb 20 11:13:26 2025 GMT
            Not After : Feb 20 11:13:26 2026 GMT
        Subject: C=US, O=Global Net Holdings Inc, CN=SHAKEN 306K
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
            Public-Key: (256 bit)
            pub:
                04:71:f2:1d:99:28:41:c1:e8:4e:2e:0d:87:62:cc:
                43:1e:ef:69:76:6e:00:ec:40:b5:e9:be:f8:c8:f6:
                59:ff:37:09:89:9c:26:84:c9:e6:83:5f:fe:a3:37:
                2a:1e:05:62:f5:c8:ab:80:93:99:55:ff:8c:95:25:
                7b:70:f7:c0:7d
            ASN1 OID: prime256v1
            NIST CURVE: P-256
        X509v3 extensions:
            1.3.6.1.5.5.7.1.26:
                0....306K
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114569.1.1.4
            X509v3 Subject Key Identifier:
                58:74:67:B9:F7:44:1B:A7:4E:F2:89:A7:02:FC:09:63:32:84:B2:B7
            X509v3 Authority Key Identifier:
                keyid:AC:D3:93:F5:43:43:CC:0A:BE:45:58:17:13:7D:92:7C:DC:C3:01:46
            X509v3 CRL Distribution Points:

                Full Name:
                    URI:https://authenticate-api.iconectiv.com/download/v1/crl

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature
            Signature Algorithm: ecdsa-with-SHA256
                30:44:02:20:27:1c:0a:0a:b9:99:08:ff:ea:d5:5b:51:d9:71:
                6e:fb:b9:aa:c1:60:f5:3c:7f:43:51:4a:56:80:65:a4:fb:9c:
                02:20:37:3a:61:7a:96:68:ab:52:e6:ff:d3:97:7e:c9:4c:72:
                e4:1f:42:81:df:09:df:93:20:f4:43:88:aa:58:ea:50
[root@ns508297 tmp]#
```

```

[root@ns508297 tmp]#
[root@ns508297 tmp]# curl https://cr.sansay.com/306K/429C7C70711E3820F0B8E1DEAE6FF3262264BFD0.pem > /tmp/certificate.txt
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left     Speed
100 2031 100 2031    0    0 3732    0 --:--:-- --:--:-- --:--:-- 3733
[root@ns508297 tmp]#
[root@ns508297 tmp]#
[root@ns508297 tmp]# openssl x509 -text -noout -in /tmp/certificate.txt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            42:9c:7c:70:71:1e:38:20:f0:b8:e1:de:ae:6f:f3:26:22:64:bf:d0
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=US, ST=California, O=Sansay Corporation, OU=Sansay CA, CN=SHAKEN Sansay Intermediate CA US WEST 1
        Validity
            Not Before: Feb 20 11:13:26 2025 GMT
            Not After : Feb 20 11:13:26 2026 GMT
        Subject: C=US, O=Global Net Holdings Inc, CN=SHAKEN 306K
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
            Public-Key: (256 bit)
            pub:
                04:71:f2:1d:99:28:41:c1:e8:4e:2e:0d:87:62:cc:
                43:1e:ef:69:76:6e:00:ec:40:b5:e9:be:f8:c8:f6:
                59:ff:37:09:89:9c:26:84:c9:e6:83:5f:fe:a3:37:
                2a:1e:05:62:f5:c8:ab:80:93:99:55:ff:8c:95:25:
                7b:70:f7:c0:7d
            ASN1 OID: prime256v1
            NIST CURVE: P-256
        X509v3 extensions:
            1.3.6.1.5.5.7.1.26:
                0....306K
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114569.1.1.4
            X509v3 Subject Key Identifier:
                58:74:67:B9:F7:44:1B:A7:4E:F2:89:A7:02:FC:09:63:32:84:B2:B7
            X509v3 Authority Key Identifier:
                keyid:AC:D3:93:F5:43:43:CC:0A:BE:45:58:17:13:7D:92:7C:DC:C3:01:46
            X509v3 CRL Distribution Points:

            Full Name:
                URI:https://authenticate-api.iconectiv.com/download/v1/crl

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature
        Signature Algorithm: ecdsa-with-SHA256
            30:44:02:20:27:1c:0a:0a:b9:99:08:ff:ea:d5:5b:51:d9:71:
            6e:fb:b9:aa:c1:60:f5:3c:7f:43:51:4a:56:80:65:a4:fb:9c:
            02:20:37:34:61:7a:96:68:4b:52:e6:ff:d3:97:7e:c9:4c:72:
            e4:1f:42:81:df:09:df:93:20:f4:43:88:aa:58:ea:50
[root@ns508297 tmp]#

```

dnis

CA

not_after

not_before

varchar

timestamp

timestamp


```

[root@ns508297 tmp]#
[root@ns508297 tmp]# curl https://cr.sansay.com/306K/429C7C70711E3820F0B8E1DEAE6FF3262264BFD0.pem > /tmp/certificate.txt
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           % Done    0     0     0       0      0      0      0      0
100 2031 100 2031    0     0 3732    0 --:--:-- --:--:-- --:--:-- 3733
[root@ns508297 tmp]#
[root@ns508297 tmp]#
[root@ns508297 tmp]# openssl x509 -text -noout -in /tmp/certificate.txt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            42:9c:7c:70:71:1e:38:20:f0:b8:e1:de:ae:6f:f3:26:22:64:bf:d0
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=US, ST=California, O=Sansay Corporation, OU=Sansay CA, CN=SHAKEN Sansay Intermediate CA US WEST 1
        Validity
            Not Before: Feb 20 11:13:26 2025 GMT
            Not After : Feb 20 11:13:26 2026 GMT
        Subject: C=US, O=Global Net Holdings Inc, CN=SHAKEN 306K
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
            Public-Key: (256 bit)
            pub:
                04:71:f2:1d:99:28:41:c1:e8:4e:2e:0d:87:62:cc:
                43:1e:ef:69:76:6e:00:ec:40:b5:e9:be:f8:c8:f6:
                59:ff:37:09:89:9c:26:84:c9:e6:83:6f:fe:a3:37:
                2a:1e:05:62:f5:c8:ab:80:93:99:55:ff:8c:95:25:
                7b:70:f7:c0:7d
            ASN1 OID: prime256v1
            NIST CURVE: P-256
        X509v3 extensions:
            1.3.6.1.5.5.7.1.26:
                0....306K
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114569.1.1.4
            X509v3 Subject Key Identifier:
                58:74:67:B9:F7:44:1B:A7:4E:F2:89:A7:02:FC:09:63:32:84:B2:B7
            X509v3 Authority Key Identifier:
                keyid:AC:D3:93:F5:43:CC:0A:BE:45:58:17:13:7D:92:7C:DC:C3:01:46
            X509v3 CRL Distribution Points:

            Full Name:
                URI:https://authenticate-api.iconectiv.com/download/v1/crl

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature
        Signature Algorithm: ecdsa-with-SHA256
            30:44:02:20:27:1c:0a:0a:b9:99:08:ff:ea:d5:5b:51:d9:71:
            6e:fb:b9:aa:c1:60:f5:3c:7f:43:51:4a:56:80:65:a4:fb:9c:
            02:20:37:34:61:7a:96:68:4b:52:e6:ff:d3:97:7e:c9:4c:72:
            e4:1f:42:81:df:09:df:93:20:f4:43:88:aa:58:ea:50
[root@ns508297 tmp]#

```

OCN

Origination

Country

varchar

varchar

varchar

```

[root@ns508297 tmp]#
[root@ns508297 tmp]# curl https://cr.sansay.com/306K/429C7C70711E3820F0B8E1DEAE6FF3262264BFD0.pem > /tmp/certificate.txt
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           % Done    0     0     0       0      0      0      0      0
100 2031 100 2031    0     0 3732    0 --:--:-- --:--:-- --:--:-- 3733
[root@ns508297 tmp]#
[root@ns508297 tmp]#
[root@ns508297 tmp]# openssl x509 -text -noout -in /tmp/certificate.txt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            42:9c:7c:70:71:1e:38:20:f0:b8:e1:de:ae:6f:f3:26:22:64:bf:d0
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=US, ST=California, O=Sansay Corporation, OU=Sansay CA, CN=SHAKEN Sansay Intermediate CA US WEST 1
        Validity
            Not Before: Feb 20 11:13:26 2025 GMT
            Not After : Feb 20 11:13:26 2026 GMT
        Subject: C=US, O=Global Net Holdings Inc, CN=SHAKEN 306K
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
            Public-Key: (256 bit)
            pub:
                04:71:f2:1d:99:28:41:c1:e8:4e:2e:0d:87:62:cc:
                43:1e:ef:69:76:6e:00:ec:40:b5:e9:be:f8:c8:f6:
                59:ff:37:09:89:9c:26:84:c9:e6:83:6f:fe:a3:37:
                2a:1e:05:62:f5:c8:ab:80:93:99:55:ff:8e:95:25:
                7b:70:f7:c0:7d
            ASN1 OID: prime256v1
            NIST CURVE: P-256
        X509v3 extensions:
            1.3.6.1.5.5.7.1.26:
                0....306K
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114569.1.1.4
            X509v3 Subject Key Identifier:
                58:74:67:B9:F7:44:1B:A7:4E:F2:89:A7:02:FC:09:63:32:84:B2:B7
            X509v3 Authority Key Identifier:
                keyid:AC:D3:93:F5:43:CC:0A:BE:45:58:17:13:7D:92:7C:DC:C3:01:46
            X509v3 CRL Distribution Points:

            Full Name:
                URI:https://authenticate-api.iconectiv.com/download/v1/crl

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature
        Signature Algorithm: ecdsa-with-SHA256
            30:44:02:20:27:1c:0a:0a:b9:99:08:ff:ea:d5:5b:51:d9:71:
            6e:fb:b9:aa:c1:60:f5:3c:7f:43:51:4a:56:80:65:a4:fb:9c:
            02:20:37:34:61:7a:96:68:4b:52:e6:ff:d3:97:7e:c9:4c:72:
            e4:1f:42:81:df:09:df:93:20:f4:43:88:aa:58:ea:50
[root@ns508297 tmp]#

```

OCN

Origination

Country

varchar

varchar

varchar

Signature	varchar
ani	varchar
dnis	varchar

```
> AC
[root@sns508297 tmp]# /opt/stirshaken/scripts/parse_identity 'eyJhbGciOiJIUzI1NiIsInR5cCI6IWR5biJlbnNpdC5kb3QwMjE1LWZvZDk6YXNjaXB1bGUiLCJ0eXAiOiJKV1QiLCJkaXZhdGEiOiJ0eXAiLCJmYWVudCI6IjE3ODIyOTQzMzMyMDA5IiwiaWF0IjoxNzQyNTYxNjUuMTU1MTQ0NDUyNTI1fSwib3JpZ2kiOiJoImQ4ZDE3NDItZGY1YS8xMmVkdWkiOjE0ODEtZWZlZjZlZjZhIn0.YW1fsALuX-QzovsR4a2T_cdIU1Wnfx1tMFhLRryZdi6OM4yeMwGvM_dAFSSdjs6SUWRNIYMObn7aZ3Rig1a;info=https://cr.sansay.com/306K/429C7C70711E3820F0B8E1DEAE6FF32622648FD0.pem';alg=ES256;ppt=shaken'
Identity:
{
  "alg": "none",
  "ppt": "shaken",
  "typ": "passport",
  "x5u": "https://cr.sansay.com/306K/429C7C70711E3820F0B8E1DEAE6FF32622648FD0.pem"
}
{
  "attest": "C",
  "dest": {
    "tn": [
      "12145463323"
    ]
  },
  "iat": 1742601603,
  "orig": {
    "tn": "15514445252"
  },
  "origid": "bd8d1742-df5a-11ed-b881-ac1f6bc6cd1a"
}

Downloading certificate...
Validating signature...
2025-03-22 10:04:29 ERROR (src/test_apps/parse_identity.c:168) [errno: 22] Signature validation failed
Certificate:
Subject CN: SHAKEN_306K;
Issuer: SHAKEN Sansay Intermediate CA US WEST 1;
Serial: 429C7C70711E3820F0B8E1DEAE6FF32622648FD0;

-----BEGIN CERTIFICATE-----
MIICQDCCAA+gAwIBAgIUqpX8cHEeOCdw0Herm/zJikv9AwCgYIKoZIzj0EAwIw
gYuXCzA3BgNVBAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybmlhbmRswGQYDVQQKDDBJT
YW5zYXkgQ29ycG9yYXRpb24xeJAQBGNVBAsMCVNhbnNheSBQDQEtcMCAGA1UEAwgn
U0hBS0V0IjFnbnNheSB3bnR1cm1IZG1hdGUgQ0EgVVMeV0VTVCAxMB4XDTI1MDIy
MDExMTMyNloXDTE1MDIyMDEyMDExMTUwRTELMAKGA1UEBHMCMCVVMxIDAeBgNVBAom
F0dsb2JhcCB0ZXQqS09sZGl1Z3MgSW5jMRQwEgYDVQQDDAtSEFLRU4gMzAzS2szB2
MBMGByqGS49AgEGCCqGSM49AwEHA0IABHhyHZkoQcHoT14Nh2LMQx7vaXzuAOxA
tem+mJjzwf83CYmcJoTJ5oNF/qM3Kh4FrvXIq4CTmVX/jJu1e3D3whZjgdsgdgw
FeYTKwYBQHUhaEcJaIoAYNB0MwNksawfVDVR0gBBawDJAMGpgghkgBhv83AQEE
MB0GA1UDQGWBRRYdGe590bbp07iacC/AIJMcSyztAfBgNVHSMEGDAGwBSs0SP1
Q0PMCr5FWbcTFzJ3MMBRjBH8gNVHR8EQDA-MDygOqA4hjZodHRwczoVL2FidGh1
bnRpY2F0ZS1hcGkuawNvbmvjdG12LnNvbS9kb3duOG9hZC92MS9jcmmwDAYDVR0T
AQH/BAlwADA0BgNVHQBAf8EBAMCB4AwCgYIKoZIzj0EAwIDRWAwRAIgJxwKCzmZ
CP/q1VtrRXFu+7mqwwD1PH9DUUpWgGWk+5wC1Dc0YXkWaeTS5v/T137JTHLK0KB
3wnfyD004iqWOpQ
-----END CERTIFICATE-----
[root@sns508297 tmp]#
```

```

Download certificate...
Validating signature#...
2026-03-22 10:04:27 ERROR (src/test_apps/parsed_identity.c:168) [errno: 22] Signature validation failed
Certificate:
    Subject CN: SHAKEN 306K;
    Issuer: SHAKEN Sansay Intermediate CA US WEST 1;
    Serial: 429C7C70711E3826F0B8E1DEAE6FF3262264BFDB;

-----BEGIN CERTIFICATE-----
MIICDCCAC+gAwIBAgIUQnp8ChHEoCDWuOHzm/z3ikj9AwGcYIKoZiiZj0EAwIw
gYuXCzAJ8nNVBAYTAlVTMRMcEQDYVQQIDApDYwpzm9ybmlHRMVSgcYVQQKB3JT
YW5zZXkgODIyYzcG9yYXRpb24xZWJlAQ8BNVBASMCVNhbNHeSBDDQTWEMCA4U1EAWwn
U0hS8BV0FI9nbhNheSB8JbnRlcml1ZGludGUpQG0gVGVmVGV0VTRVCXAxBADXTII1MDIY
MDEXMtMYNlloXDITIMDIYMdEXMtMYNlwoRTELMAKA6U1EBhMCVVXkIDAeBgNVBAWA
FDbsdzJhbcCB0ZXQ5SG9sZGluzMGSw5jMRQwGEYDVQDDDAITSEFLRUqGAzA2S2BZ
MBMGBYqGSMA4RGAGGCCqGSM49AwEHAIIBAHhyHkoCoHoTI4Nh2LMQv7aX2uAOAx
tem++MjZf83CYmcJotJ35onF/qM3Kh4FYiXq4TCMVX/jJUle3D3WH2jsgsdwgdd
FGYIKWBBOUHARoECJAioAYWBDMNksWfwYDVRBgBAwdjAMBggpgkh8hv8AJAGEE
MBGA6LUdgdbQBRYGde590Qbp07ylacC/AljMoSyztAF8BNVHSMEDGAWBS86SP1
QP8PZ5FWbCTZ383MMWRj3BHgnVHREBGDA+MDYp0QAghJZoIdHwczovL2Fi6dh1
bNrYFZ3ZDR1bmVucyVubWVkdGl2LmV5b3k3dUB9NzC9Z2MS9jcmmDAYDVR8RT
AQH/BIAIwADA0AB8BNHBQBAF8EBAMCBRAwCgYIKoZIj0EAwIDRWArCmAznjKCWRCZ
CP/q1vTR2FXu7+mqqwD1PH9DUlpwgGkw+5wcDIOXYQWaet55v/Tl37ZTHLKHK0K
3wnfkYDQ04iqWOpQ
-----END CERTIFICATE-----
[root@ns508297 tmp]#

```

Field Name	Type
Identity_error	varchar

How to get Email address to send email to:

```
stilog=# select * from sp limit 10;
```

id	type	company	status	first_name	last_name	email	phone
100769	Service Provider	Zultys Inc.	Active	Pavel	Matsienok	sti-pa@zultys.com	408-328-0450
100645	Service Provider	BlueRiver Communic...	Active				
101880	Service Provider	Dell Telephone Coo...	Active	DTC	NOC		915-964-2163
101660	Service Provider	@Link Services LL...	Active	Rajendrakumar...	Veerappan	raj@atlink.net	405-753-7151
101959	Service Provider	011 Telecom LLC	Active	Ricardo	Gonzalez	noc@011telecom.com	
101956	Service Provider	1 CALL CONNECT	Active			noc@1callconnect.net	
101666	Service Provider	1 Point Communicat...	Active	Matt	Campbell	mcampbell@1pointcom.com	540-627-6506
100889	Service Provider	101Netlink	Active	Seth	Johannesen	voip@101netlink.com	707-923-4000 (500)
100834	Service Provider	101VOICE	Active	Arman	Eghbali	compliance@101voice.com	408-204-8000
100254	Service Provider	123.Net Inc	Active	Support		support@123.net	248-228-8200 (1)

(10 rows)

```
stilog=#
```

How to push to mattermost

<https://mattermost.denovolab.com/hooks/fiwxfytpn3rxmdjn1ff55iagao>

javascript

Copy

Edit

```
const axios = require('axios');

const webhookUrl = 'https://mattermost.denovolab.com/hooks/fiwxfytpn3rxmdjn1ff55iagao';

// Create the message payload
const payload = {
  text: "🚀 Hello, Mattermost! This is a test event from Node.js."
};

// Send the POST request
axios.post(webhookUrl, payload)
  .then(response => {
    console.log('✅ Event sent successfully:', response.status);
  })
  .catch(error => {
    console.error('❌ Error sending event:', error.message);
  });
```

Table: email_event

Field Name	Type	Description
uuid	uuid	This is auto generated key
email	varchar	Where we sent to
subject	varchar	
content	varchar	
opt_out	boolean	

Table: opt_out_company

Field Name	Type	Description
uuid	uuid	This is auto generated key
company	varchar	The company that wanted to opt out
timestamp	time	Auto generated with now()

- We need opt-out api: api.stilog.peeringhub.io/rm/{email_uuid}
- When user click on the opt-out link, then we insert to this table.
- We should not send email again to this same company

Email content

Subject: Notification: Invalid Identity SHAKEN for OCN xxx

Content:

Hi <first_name>,

This is a **courtesy email** to inform you that we have detected your OCN **xxx** is generating an **invalid identity header**. The identity header in question is:

```
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9jci5zYW5zYXkuY29tLzMwNksvNDI5QzdDNzA3MTFFMzgyMEYwQjhFMURFQUU2RkYzMjYyMjY0QkZEMC5wZW0ifQ.eyJhdHRlc3QiOiJDIiwiaGVhZCI6eyJ0biI6WyIxMjE0NTQ2MzMyMyJdfSwiaWF0IjoxNzQyNjAxNjAzLCJvcmlnIjp7InRuIjoimTU1MTQ0NDUyNTIifSwib3JpZ2lkIjoimQ4ZDE3NDItZGY1YS0xMWVklWI4ODEtYWMxZjZiYzZjZDFhIn0.OYwifsALuX-QzovsR4a2T_cd1UMLWNfx1tMFhLRRyZdi60M4yeMwGvM_dAfS5dJs65UWRNIYmM0Bn7aZ3RigiA;info=<https://cr.sansay.com/306K/429C7C70711E3820F0B8E1DEAE6FF3262264BFD0.pem>;alg=ES256;ppt=shaken
```

Error:



Signature validation failed

As **Peeringhub** is a **certified STIR/SHAKEN CA**, we can generate a **valid certificate** for you to resolve this issue.

♦ **Pricing:**

Email content

3 Configure Nodemailer to Use .hbs Templates

Create a `sendEmail.js` file:

```
javascript Copy Edit

const nodemailer = require('nodemailer');
const hbs = require('nodemailer-express-handlebars');
const path = require('path');

// Step 1: Configure Nodemailer Transporter
const transporter = nodemailer.createTransport({
  service: 'gmail', // or use SMTP settings
  auth: {
    user: 'your-email@gmail.com',
    pass: 'your-email-password'
  }
});

// Step 2: Configure Handlebars Templating Engine
transporter.use('compile', hbs({
  viewEngine: {
    extname: '.hbs',
    partialsDir: path.join(__dirname, 'views/emails'),
    defaultLayout: false,
  },
  viewPath: path.join(__dirname, 'views/emails'),
  extName: '.hbs'
}));

// Step 3: Send Email
```

Pls don't hard code the email content. Pls use .hbs to generate it dynamically.

Type of error - email

- Need to support different email content / subject for different type of error:
 - Invalid Certificate
 - Certificate Not Downloaded
 - Invalid Identity
 - Expired Certificate

Not found means the url is not found

```
[Not Found[root@ns508297 tmp]#  
[[root@ns508297 tmp]# https://cr.sansay.com/306K/429C7C70711E3820F0B8E1D429C7C70711E3820F0B8E1DEAE6FF3262264BFD0.pem  
-bash: https://cr.sansay.com/306K/429C7C70711E3820F0B8E1D429C7C70711E3820F0B8E1DEAE6FF3262264BFD0.pem: No such file or directory  
[root@ns508297 tmp]# █
```

Logging

What to do

- We should have daily log file
- All activity should be logged in log file

Server side logging

[YYYY-MM-DD hh:mm:ss] Receive error log {xxxx}. Assign UUID xxx

[YYYY-MM-DD hh:mm:ss] UUID XXX is not a new log for yyyy-mm-dd. Insert to DB and ignore.

[YYYY-MM-DD hh:mm:ss] UUID XXX is a new log for yyyy-mm-dd.

[YYYY-MM-DD hh:mm:ss] Send Notification Email to XXXX@dd.com | subject: ... | Content ...

[YYYY-MM-DD hh:mm:ss] Push Notification Email to Mattermost

[YYYY-MM-DD hh:mm:ss] Insert email event to Postgres

Client side logging

[YYYY-MM-DD hh:mm:ss] Found error log xxxxx. Push to server. Receive UUID xxxx

Config file

Server side .env

```
Postgres_ip:  
postgres_host:  
postgres_db:  
postgres_user:  
Postgres_pass:  
Mattermost_ur:  
From_email  
From_mail_ip  
From_mail_port  
Cc_email:  
From_mail_passport  
Log_path:  
enable_auto_email:
```

Client side .env

```
Src_log_path:  
server_url:
```

Admin API needed

Auth

GET /auth

- User
- Pass

Return token

GET error

GET /admin/get_error

- Start_time
- End_time
- Unique (true = only return repeated='f', false = only return repeated='t')

POST /admin/error/{error_uuid}/send_alert

GET /admin/error/{error_uuid}

API needed

GET /admin/error/{error_uuid}/email

- Return the to_email, subject, content

How we want to use it

- At the beginning, we will have admin to manual check each error and use send_email aPI to send after using get_email api to review the content.
- After we feel it is working, then we turn on auto_email to let the program to send manually.

Table: admin_auth

Field Name	Type	Description
uuid	varchar	
email	varchar	
password	varchar	

Log search

Start time

End time

Repeated

☐

Time	Identity Header	Action

Actions:

- View Identity Detail
- Send Alert
- Preview Alert Email