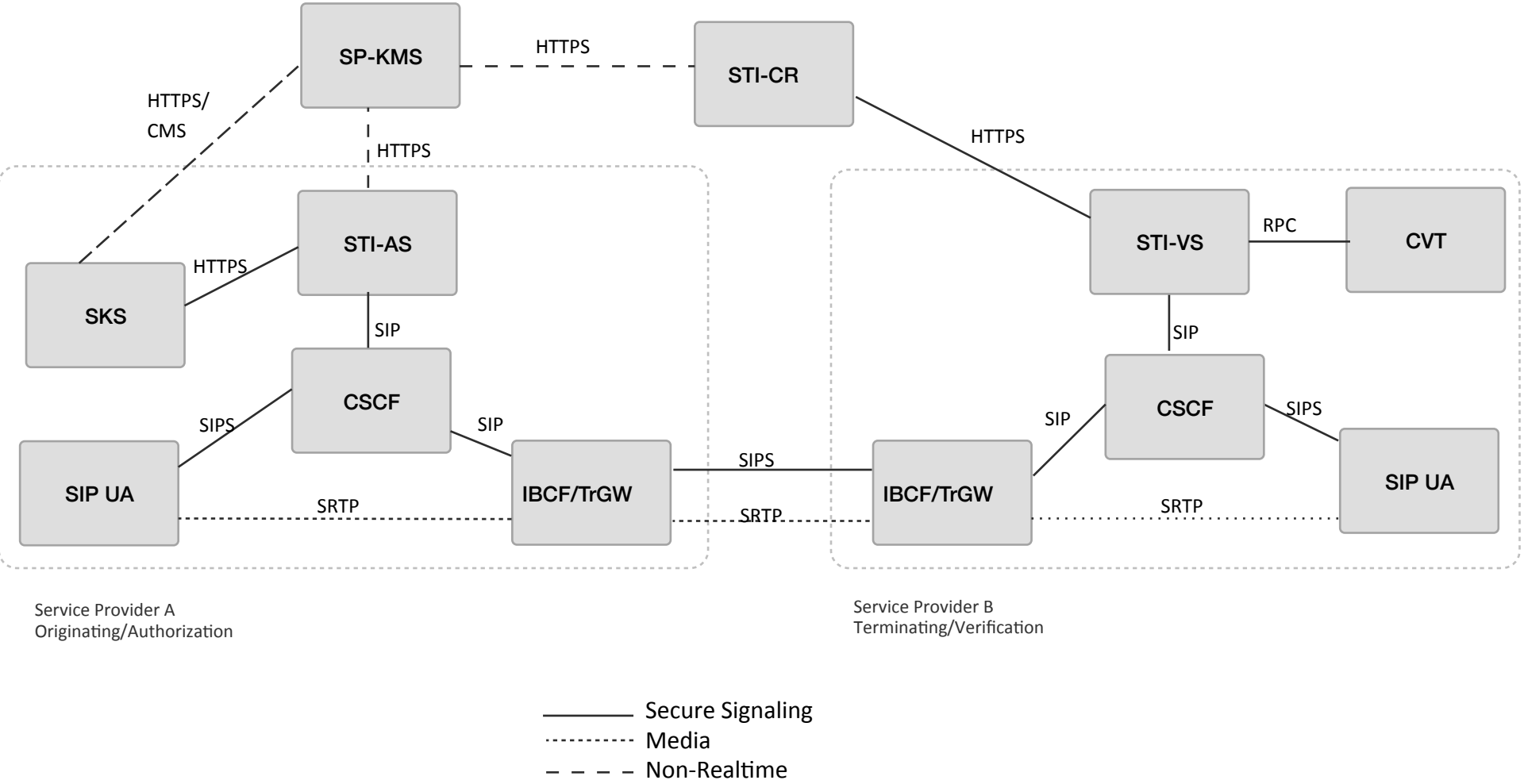
SHAKEN
STI-AS and STI-VS Overview with API

ATIS-1000074
ATIS-1000080
IPNNI-2017-00021R004
IPNNI-2017-00089R000

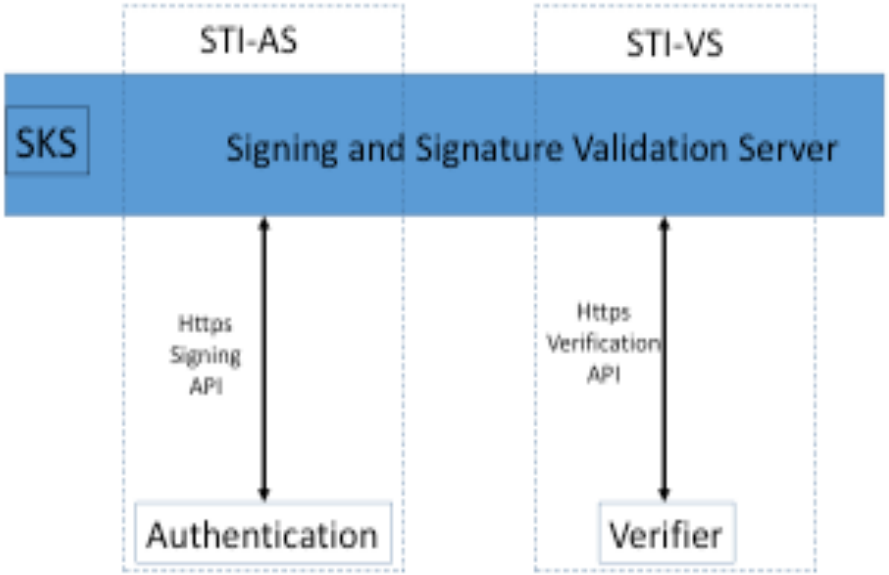
Overview

- Architecture
- API for Authenticator and Verifier <-> SSVS
- Detailed call flows using API
- Backup – call flows without API

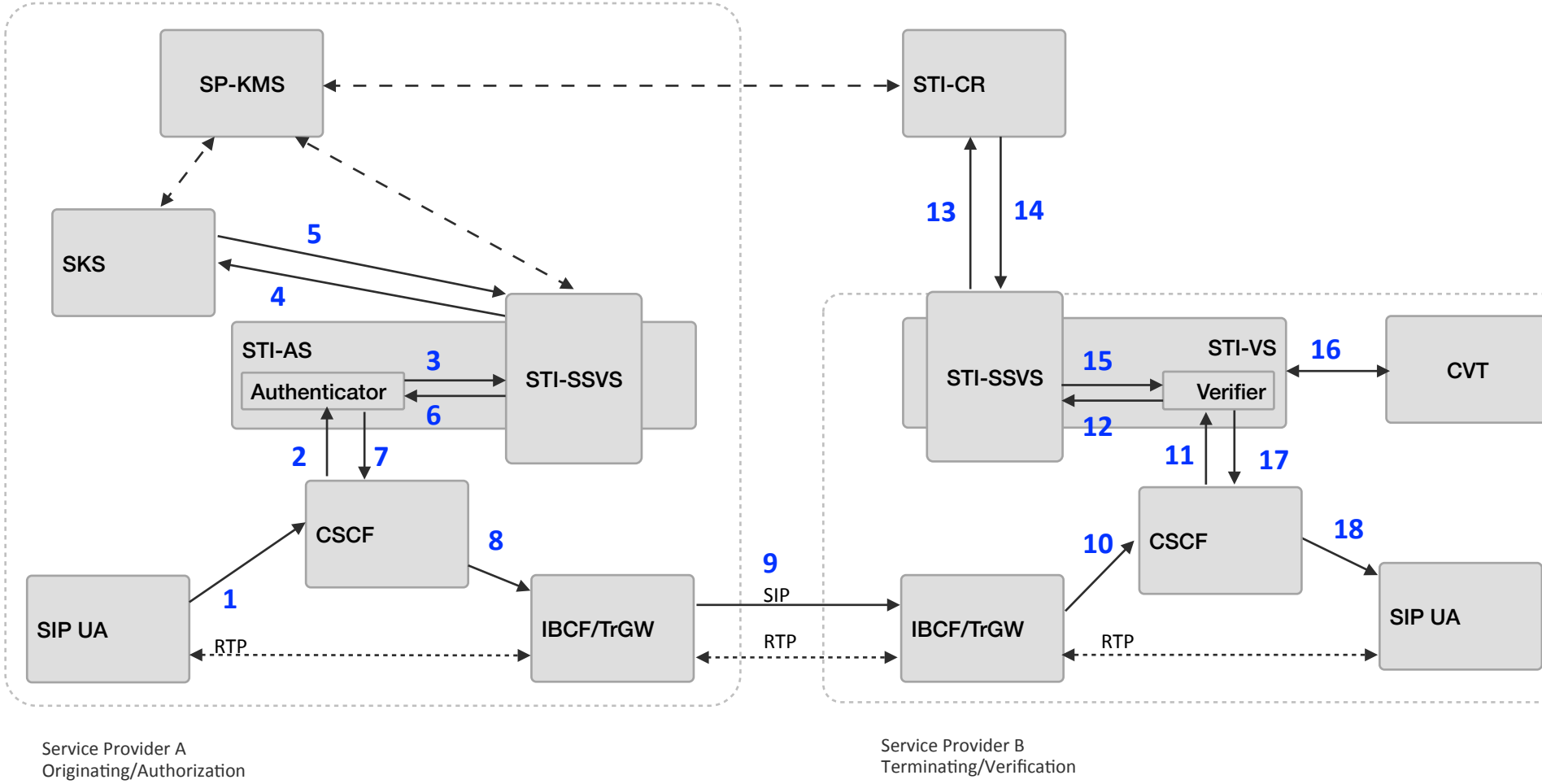


Secure Signaling
Media
Non-Realtime

Signing and Signature Validation Server



STI Call Origination & Termination



Call Flow Steps

1. The originating SIP UA, which first REGISTERs and is authenticated to the CSCF, creates a SIP INVITE with a telephone number identity.

2. The CSCF of the originating provider adds a P-Asserted-Identity header field asserting the telephone number of the originating SIP UA. The CSCF then triggers the Authenticator in the STI-AS.

3. The Authenticator in the originating SP network (i.e., Service Provider A) first determines through service provider specific means the legitimacy of the telephone number identity being used in the INVITE. The Authenticator sends a signing request to the STI-SSVS.

4. The STI-SSVS then securely requests its private key from the SKS.

5. The SKS provides the private key in the response, and the STI-SSVS signs the Identity header field per RFC draft-ietf-stir-4474bis using the originating telephone number in the P-Asserted-Identity header field.

6. The STI-SSVS returns the signed SIP Identity header field to the Authenticator.

7. The Authenticator passes the INVITE back to the SP A's CSCF.

8. The originating CSCF, through standard resolution, routes the call to the egress IBCF.

9. The INVITE is routed over the NNI through the standard inter-domain routing configuration.

10. The terminating SP's (Service Provider B) ingress IBCF receives the INVITE over the NNI.

11. The terminating CSCF triggers the STI-VS Verifier. The STI-VS Verifier must be invoked before terminating call processing.

12. The Verifier sends a verification request to the STI-SSVS.

13. The STI-SSVS uses the "info" parameter information in the Identity header field per RFC 4474bis to determine the STI-CR URI and makes an HTTPS request to the STI-CR.

14. The STI-SSVS validates the certificate received from the STI-CR and then extracts the public key. It constructs the RFC 4474bis format and uses the public key to verify the signature in the Identity header field, which validates the Caller ID used when signing the INVITE on the originating service provider STI-AS.

15. The STI-SSVS sends a response to the Verifier indicating whether the identity has been verified.

16. The CVT is an optional function that can be invoked to perform call spam analytics or other mitigation techniques and return a response related to what should be signaled to the user for a legitimate or illegitimate call. The CVT may be integrated in the service provider network or outside the service provider network by a third party.

17. Depending on the result of the STI validation, the STI-VS determines that the call is to be completed with an appropriate indicator and the INVITE is passed back to the terminating CSCF which continues to set up the call to the terminating SIP UA.

18. The terminating SIP UA receives the INVITE and normal SIP processing of the call continues, returning "200 OK" or optionally setting up media end-to-end.

STI-AS & STI-VS RESTful web services

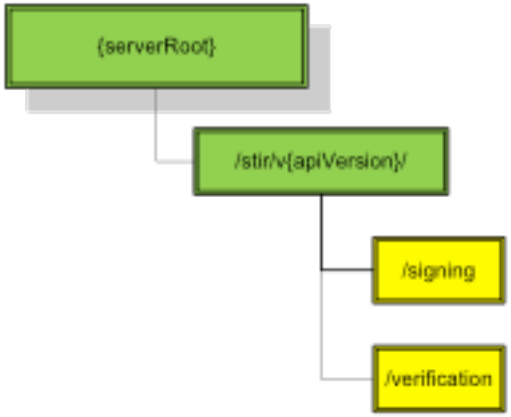
- STI-AS and STI-VS expose a RESTful web service - Signing and Signature Verification Service (SSVS).
- Implemented using HTTP and aligned with the principles of RESTful API.
- Only JSON based data format is supported.
  - APIs use "application/json" content type
- POST HTTP request is used for the both APIs.
- HTTP 1.1 protocol version has to be supported by server side.

REST resource structure

- REST resources are defined with respect to a “server Root” :

  “serverRoot” = http://{hostname}:{port}/{optionalRoutingPath}

- The resource structure is provided below:



HTTP Request (POST) headers

Header Name	Mandatory?	Description
X-RequestID	N	According to the general agreement the transaction UUID should be published by component calling an exposed by other component API in order to make possible the transaction traceability in case of troubleshooting and fault analysis. Generated UUIID should be compliant with RFC 4122. If received will not be validated explicitly by server. If not received it will be automatically generated by STI-AS/VS service on request receipt. Received/Generated transaction UUID will be returned back in the corresponding HTTP response in “X-RequestID” header.
X-InstanceID	N	For auditing purpose each component calling the API should identify itself by sending its identity (e.g. Instar name , VNFC name/UUID , VM name/UUID ...) in "**X-InstanceID**" header .
Content-Type	Y	Determines the format of the request body. Valid value is: “**application/json**”. Requests with other types will be rejected with “415 Unsupported Media type” HTTP status code.
Accept	N	If specified has to contain “**application/json**” content type, otherwise HTTP request will be rejected with “406 Not Acceptable“ HTTP Status Code. If not specified will be y default handled as “**application/json**”.

HTTP Response headers

Header Name	Mandatory?	Description
X-RequestID	Y	Received/Generated transaction UUID will be returned back in the corresponding HTTP response.
Content-Type	Y	Determines the format of the response body. Valid value is : **"application/json"**

Datatype: signingRequest

Key Name	Key Value Type	Required?	Description
attest	String Allowed values : ["A" , "B" , "C"]	Y	SHAKEN extension to PASSporT. Indicator identifying the service provider that is vouching for the call as well as a clearly indicating what information the service provider is attesting to. SHAKEN spec requires "attest" key value be set to uppercase characters "A", "B", or "C".
dest	destTelephoneNumber	Y	Represents the called party. Array containing **one or more** identities of telepnoneNumber type.
iat	Integer	Y	"Issued At Claim": Should be set to the date and time of issuance of the PASSporT Token. The time value should be in the Numeric Date format defined in RFC 7519 : number of seconds elapsed since 00:00:00 UTV , Thursday , 1 January 1970 not including leap seconds .
orig	origTelephoneNumber	Y	Represents the asserted identity of the originator of the personal communications signaling.
origid	String	Y	The unique origination identifier ("origid") is defined as part of SHAKEN extension to PASSporT. This unique origination identifier should be a globally unique string corresponding to a UUID (RFC 4122). Note: VM UUID can be used as a unique originator identifier.

Note: API assumes ES256 as the algorithm

Datatype: origTelephoneNumber

Field	Type	Required ?	Description
tn	String Allowed Characters : [0-9] ,*,#,+, and visual separators defined in RFC 3966 : “.”, “-“, “(“, “)”.	Y	Telephone Number of Originating/Destination identity. Server will remove all non-numeric characters if received except start (*) and pound (#) characters. Ex. : (+1)235-555-1212 → 12355551212

Datatype: destTelephoneNumber

Field	Type	Required ?	Description
tn	List of Strings [1 … unbounded] Allowed Characters : [0-9] ,*,#,+, and visual separators defined in RFC 3966: “.”, “-“, “(“, “)”.	Y	List containing **one or more** identities of String type. Server will remove all non-numeric characters if received except start (*) and pound (#) characters. Ex. : (+1)235-555-1212 → 12355551212

Datatype: signingResponse

Key Name	Key Value Type	Required?	Description
identity	String Cannot be NULL	Y	Identity header value as defined in RFC4474bis with “identityDigest” in full format and mandatory “info” header parameter .“info” parameter will contain the public key URL of the certificate used during STI signing.

Datatype: verificationRequest

Key Name	Key Value Type	Required ?	Description
identity	String	Y	Identity header value as defined in RFC4474bis with "identityDigest" in full format and mandatory "info" header parameter.
dest	destTelephoneNumber	Y	Represents the **or more** identities
iat	Integer	Y	"Issued At Cla time of issuanc The time va format defined elapsed since 1970 not includ
orig	origTelephoneNumber	Y	Represents the the personal c

This should be the value of "To:" header field parameter in the incoming Invite

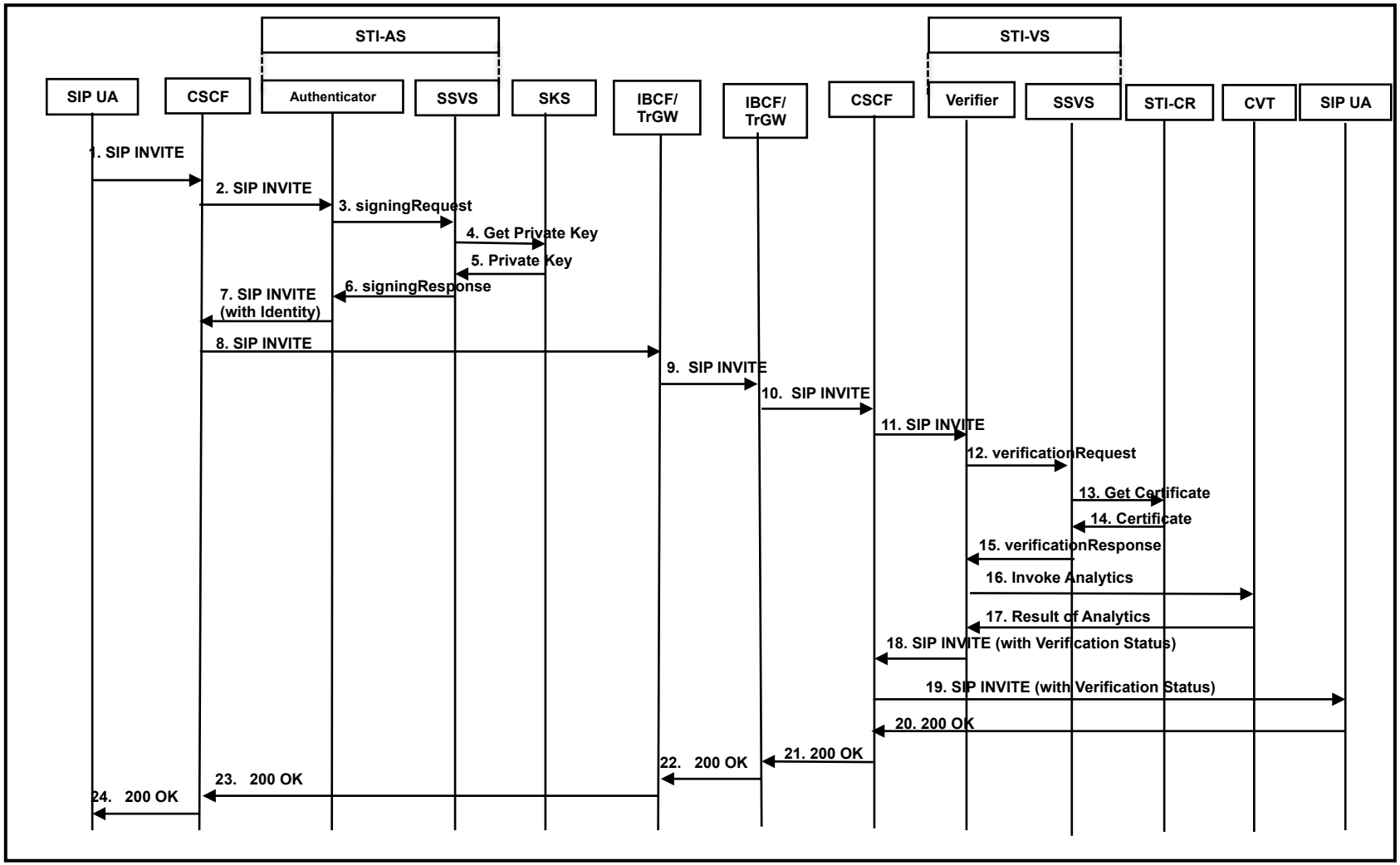
This should be the value of the Date header field parameter in the incoming Invite.

This should be the value in the "P-Asserted-Identity" or "From" header field parameter in the incoming Invite.

Datatype: verificationResponse

Key Name	Key Value Type	Required?	Description
reasoncode	Integer	N	Reason Code to be used in case of failed verification by STI-VS to build SIP Reason header if required. Currently possible values are defined as follows (please pay attention they can be extended/changed in the future) : 403,428 (will not be returned in the initial release) ,436,437,438 403 – "Stale Date header received" 436 – Bad Public Key Certificate URI
reasontext	String	N	Reason Text to be used in case of failed verification by STI-VS to build SIP Reason header if required. Currently possible values are defined as follows (please pay attention they can be extended/changed in the future) : 403 - "Stale Date" 428 - "Use Identity Header" (will not be returned in the initial release) 436 – "Bad Identity Info" 437 – "Unsupported Credential" 438 – "Invalid Identity Header"
reasondesc	String	N	Reason details description . Can be used for logging and troubleshooting.
verstat	String {"TN-Validation-Passed", "TN-Validation-Failed", "No-TN-Validation"}	Y	Verification Status : **TN-Validation-Passed** - The calling number passed the validation **TN-Validation-Failed** - The calling number failed the validation **No-TN-Validation** - No validation number was performed

End-to-End STI Call Origination & Termination



Information/control flow for CM

1. The originating SIP UA sends a SIP INVITE request with a tel URI in the From header field parameter.

2. The CSCF of the originating provider adds a P-Asserted-Identity header field for the originating SIP UA. After initial call processing, the CSCF then initiates an originating trigger to the STI-AS for the INVITE.

3. The authenticator parses the SIP INVITE and sends a signingRequest to the SSVS.

4. The SSVS then securely requests its private key from the SKS.

5. The SKS provides the private key in the response, and the SSVS builds the PASSporT using the JWT populated from the information in the signingRequest received from the Authenticator. The SSVS signs the PASSport using the private key .

6. The SSVS sends the PASSporT and a link to the public key certificate in a signingResponse to the Authenticator

7. The Authenticator builds the SIP Identity header field using the Identity information returned from the SSVS. The Authenticator then returns the INVITE back to SP A's CSCF.

8. The originating CSCF, through standard resolution, routes the call to the egress IBCF.

9. The INVITE is routed over the NNI through the standard inter-domain routing configuration.

10. The terminating SP's (Service Provider B) ingress IBCF receives the INVITE over the NNI and forwards to the CSCF.

11.The terminating CSCF initiates a terminating trigger to the Verifier in the STI-VS for the INVITE before terminating call processing.

12. The Verifier extracts the Identity header field from the SIP INVITE and sends a verificationRequest to the SSVS.

Information/control flow for CM

13. The SSVS uses the “info” parameter header field parameter in the Identity header field per draft-ietf-stir-4474bis to determine the STI-CR URI and makes an HTTPS request to the STI-CR to get the public key certificate.

14. The SSVS validates the certificate (see Section 5.3.1 of the SHAKEN framework for details) and then extracts the public key. It constructs the format as defined in draft-ietf-stir-4474bis and uses the public key to verify the signature in the Identity header field, which validates the caller ID used when signing the INVITE on the originating service provider STI-AS.

15. The SSVS returns the results of the verification by sending a verificationResponse sent to the Verifier.

16. The CVT is an optional function that can be invoked by the Verifier to perform call spam analytics or other mitigation techniques The CVT may be integrated in the service provider network or outside the service provider network by a third party.

17. The CVT returns a response related to what should be signaled to the user for a legitimate or illegitimate call.

18. Depending on the result of the STI validation, the Verifier determines that the call is to be completed using the “verstat” URI parameter and the SIP INVITE is passed back to the terminating CSCF, including any Call-Info values as defined in draft-ietf-sipcore-callinfo-spam. The CSCF continues to set up the call to the terminating SIP UA.

19. The terminating SIP UA receives the INVITE and uses the Call-Info values to display an indication on the user’s device with reflective of the values in the Call-Info. Normal SIP processing of the call continues, returning a SIP 200 OK response.

20-24. The SIP 200 OK response is sent to the originating UA and media is setup end-to-end.

Step 5

a) Construct the PASSporT JWS elements

- Construct the JWS Protected header
- Construct the JWS Payload

b) Generate JSON Web Signature over the PASSporT using the private key and the specified algorithm.

- See draft-ietf-stir-passport Appendix A for a step by step example.

Step 7

Build SIP Identity header field (example on the next slide):

- signed PASSporT from step 5b.
- “info” header field parameter MUST match the “x5u” parameter in the PASSport
- “alg” header field parameter MUST match the “alg” in the PASSporT

Example SIP INVITE

```
INVITE sip:+12155551213@tel.example1.net SIP/2.0
Via: SIP/2.0/UDP 10.36.78.177:60012;branch=z9hG4bK-524287-1---77ba17085d60f141;rport
Max-Forwards: 69
Contact: <sip:+12155551212@69.241.19.12:50207;rinstance=9da3088f36cc528e>
To: <sip:+19299100814@provteam.in>
From: <sip:+19299100813@provteam.in>;tag=614bdb40
Call-ID: 79048YzkxNDA5NTI1MzA0OWFjOTFkMmFlODhiNTI2OWQ1ZTI
P-Asserted-Identity: <sip:+19299100814@provteam.in>
CSeq: 2 INVITE
Allow: SUBSCRIBE, NOTIFY, INVITE, ACK, CANCEL, BYE,
REFER, INFO, MESSAGE, OPTIONS
Content-Type: application/sdp
Date: Tue, 16 Aug 2016 19:23:38 GMT
Identity: eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0Iiwic
HB0Ijoic2hha2VuIiwieDV1IjoiaHR0cDovL2NlcnQtYXV0aC5
wb2Muc3lzLmNvbWNhc3QubmV0L2V4YW1wbGUuY2Vyd
CJ9eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6IisxMjE1NTU1M
TIxMyJ9LCJpYXQiOiIxNDcxMzc1NDE4Iiwib3JpZyI6eyJ0biI6
4oCdKzEyMTU1NTUxMjEyIn0sIm9yaWdpZCI6IjEyM2U0N
TY3LWU4OWItMTJkMy1hNDU2LTQyNjY1NTQ0MDAwMC
J9._28kAwRWnheXyA6nY4MvmK5JKHZH9hSYkWI4g75mn
q9Tj2lW4WPm0PlvudoGaj7wM5XujZUTb_3MA4modoDtCA;
info=<http://cert.provteam.in/example.cert>;alg=ES256
Content-Length: 153
v=0
o=- 13103070023943130 1 IN IP4 10.36.78.177
c=IN IP4 10.36.78.177
t=0 0
m=audio 54242 RTP/AVP 0
a=sendrecv
```

Step 5a. JWS Token/PASSporT

JWS Protected header :

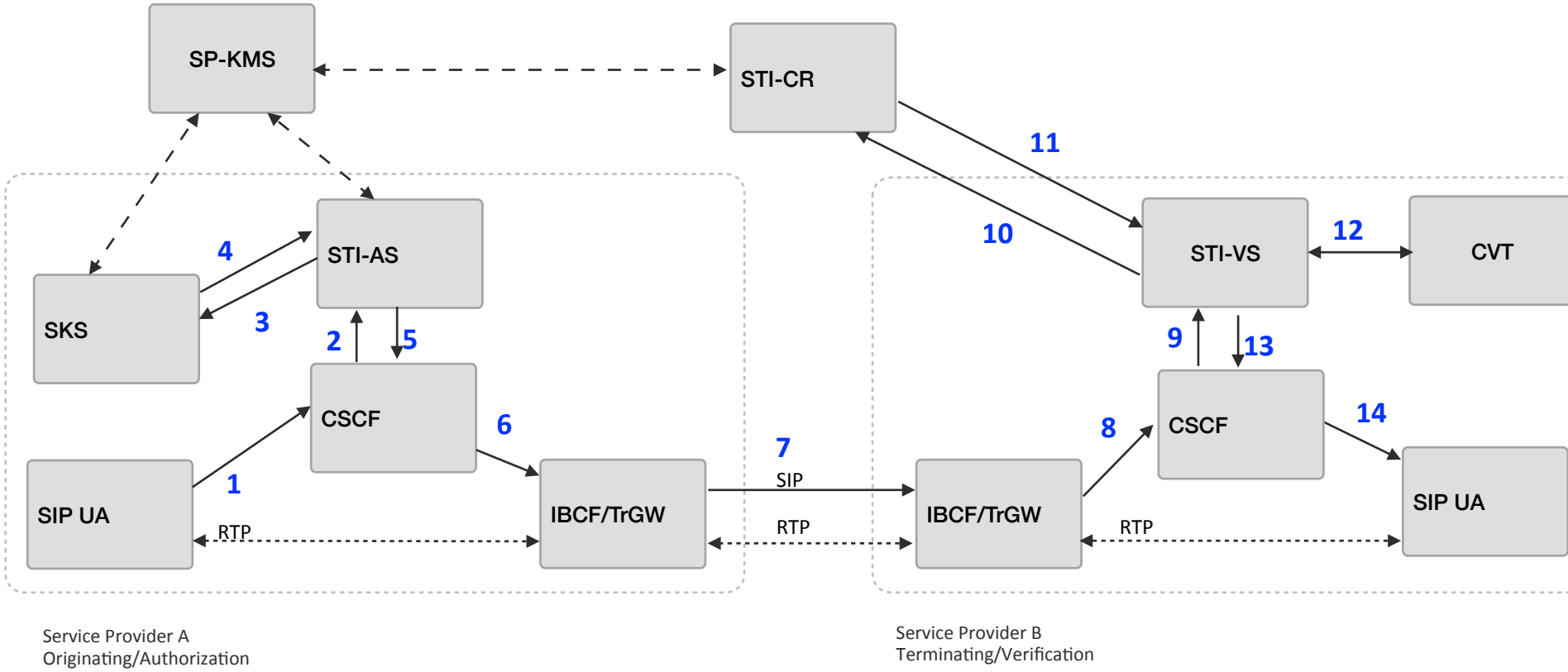
```
{"alg":"es256",
"typ":"passport",
"ppt":"shaken",
"x5u":"https://cert.cr.provteam.in/example.cert>"
}
```

JWS Payload (JWT claims) :

```
{"attest":"A",
 "dest":{"tn":["19299100814"]},
 "iat":1443208345,
 "orig":{"tn": "19299100813"},
 "origid":" 123e4567-e89b-12d3a456-426655440000 "
 }
```

Backup

STI Call Origination & Termination – Target for Prototype



Call Flow Steps

1. The originating SIP UA, which first REGISTERs and is authenticated to the CSCF, creates a SIP INVITE with a telephone number identity.

2. The CSCF of the originating provider adds a P-Asserted-Identity header field asserting the Caller ID of the originating SIP UA. The CSCF then initiates an originating trigger to the STI-AS for the INVITE. The STI-AS is invoked after originating call processing.

3. The **STI-AS** in the originating SP (i.e., Service Provider A) first determines through service provider specific means the legitimacy of the telephone number identity being used in the INVITE. The STI-AS then securely requests its private key from the SKS.

4. The SKS provides the private key in the response, and the STI-AS signs the INVITE and adds an Identity header field per RFC draft-ietf-stir-4474bis using the Caller ID in the P-Asserted-Identity header field.

5. The STI-AS passes the INVITE back to the SP A's CSCF.

6. The originating CSCF, through standard resolution, routes the call to the egress IBCF.

7. The INVITE is routed over the NNI through the standard inter-domain routing configuration.

8. The terminating SP's (Service Provider B) ingress IBCF receives the INVITE over the NNI.

9.The terminating CSCF initiates a terminating trigger to the STI-VS for the INVITE. The STI-VS must be invoked before terminating call processing.

10. The terminating SP STI-VS uses the "info" parameter information in the Identity header field per RFC 4474bis to determine the STI-CR URI and makes an HTTPS request to the STI-CR.

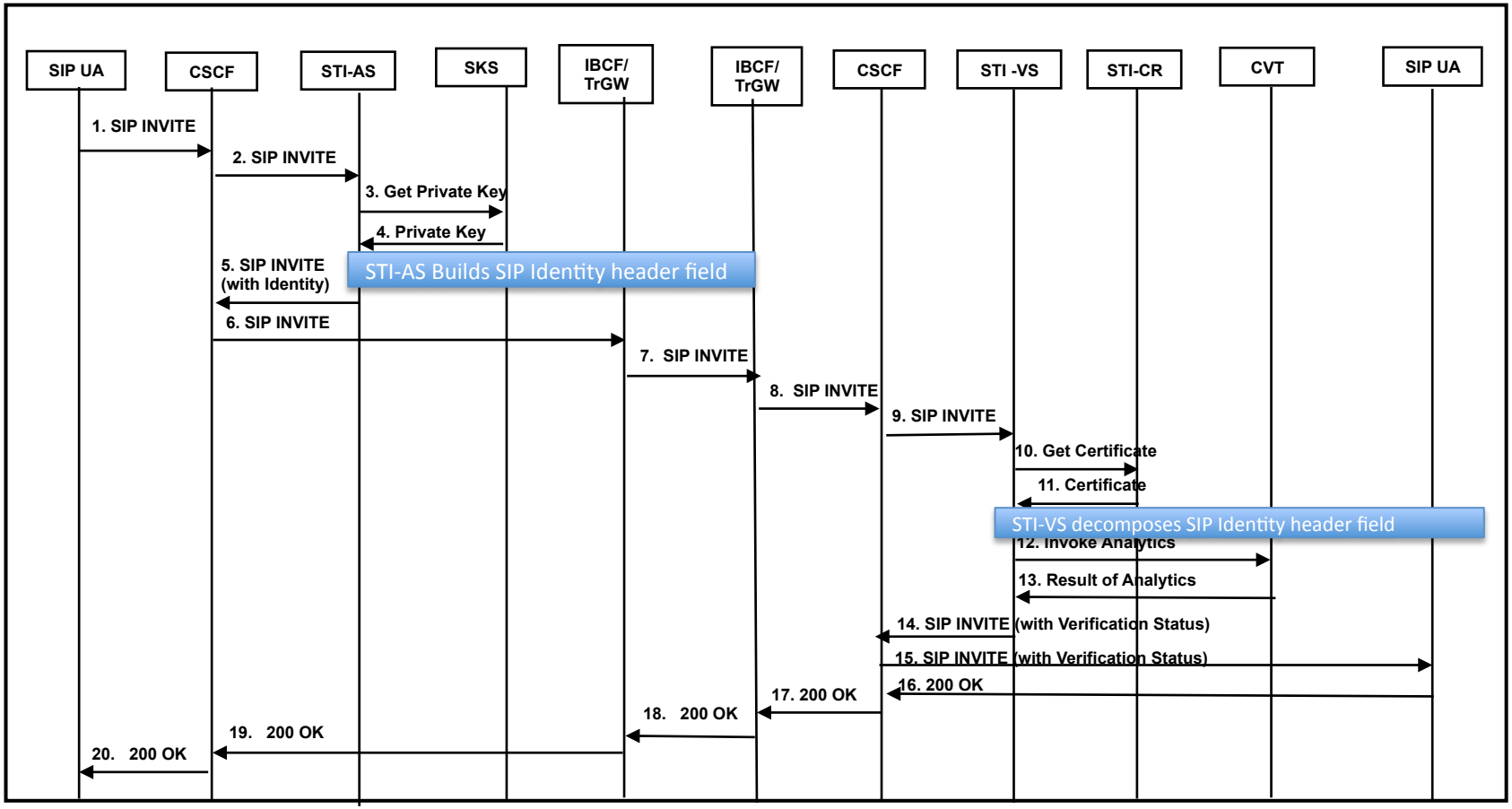
11. The STI-VS validates the certificate and then extracts the public key. It constructs the RFC 4474bis format and uses the public key to verify the signature in the Identity header field, which validates the Caller ID used when signing the INVITE on the originating service provider STI-AS.

12. The CVT is an optional function that can be invoked to perform call spam analytics or other mitigation techniques and return a response related to what should be signaled to the user for a legitimate or illegitimate call. The CVT may be integrated in the service provider network or outside the service provider network by a third party.

13. Depending on the result of the STI validation, the STI-VS determines that the call is to be completed with an appropriate indicator and the INVITE is passed back to the terminating CSCF which continues to set up the call to the terminating SIP UA.

14. The terminating SIP UA receives the INVITE and normal SIP processing of the call continues, returning "200 OK" or optionally setting up media end-to-end.

End-to-End STI Call Origination & Termination



Information/control flow for CM

1. The originating SIP UA sends a SIP INVITE request with a tel URI in the From header field parameter.

2. The CSCF of the originating provider adds a P-Asserted-Identity header field for the originating SIP UA. After initial call processing, the CSCF then initiates an originating trigger to the STI-AS for the INVITE.

3. The STI-AS then securely requests its private key from the SKS.

4. The SKS provides the private key in the response, and the STI-AS adds an Identity header field per RFC per draft-ietf-stir-4474bis. The From header field parameter from the initial SIP INVITE is used in the P-Asserted-Identity header field.

5. The STI-AS passes the INVITE back to the SP A's CSCF.

6. The originating CSCF, through standard resolution, routes the call to the egress IBCF.

7. The INVITE is routed over the NNI through the standard inter-domain routing configuration.

8. The terminating SP's (Service Provider B) ingress IBCF receives the INVITE over the NNI and forwards to the CSCF.

9.The terminating CSCF initiates a terminating trigger to the STI-VS for the INVITE before terminating call processing.

10. The terminating SP STI-VS uses the "info" parameter header field parameter in the Identity header field per draft-ietf-stir-4474bis to determine the STI-CR URI and makes an HTTPS request to the TN-CR to get the public key certificate.

11. The STI-VS validates the certificate (see Section 5.3.1 of the SHAKEN framework for details) and then extracts the public key. It constructs the format as defined in draft-ietf-stir-4474bis and uses the public key to verify the signature in the Identity header field, which validates the caller ID used when signing the INVITE on the originating service provider STI-AS.

12. The CVT is an optional function that can be invoked to perform call spam analytics or other mitigation techniques The CVT may be integrated in the service provider network or outside the service provider network by a third party.

13. The CVT returns a response related to what should be signaled to the user for a legitimate or illegitimate call.

14. Depending on the result of the STI validation, the STI-VS determines that the call is to be completed with an appropriate indicator and the SIP INVITE is passed back to the terminating CSCF, including any Call-Info values as defined in draft-sipcore-callinfo-spam. The CSCF continues to set up the call to the terminating SIP UA.

15. The terminating SIP UA receives the INVITE and uses the Call-Info values to display an indication on the user's device with reflective of the values in the Call-Info. Normal SIP processing of the call continues, returning a SIP 200 OK response.

16-20. The SIP 200 OK response is sent to the originating UA and media is setup end-to-end.