SHAKEN- Centralized Authentication and Verification Server API

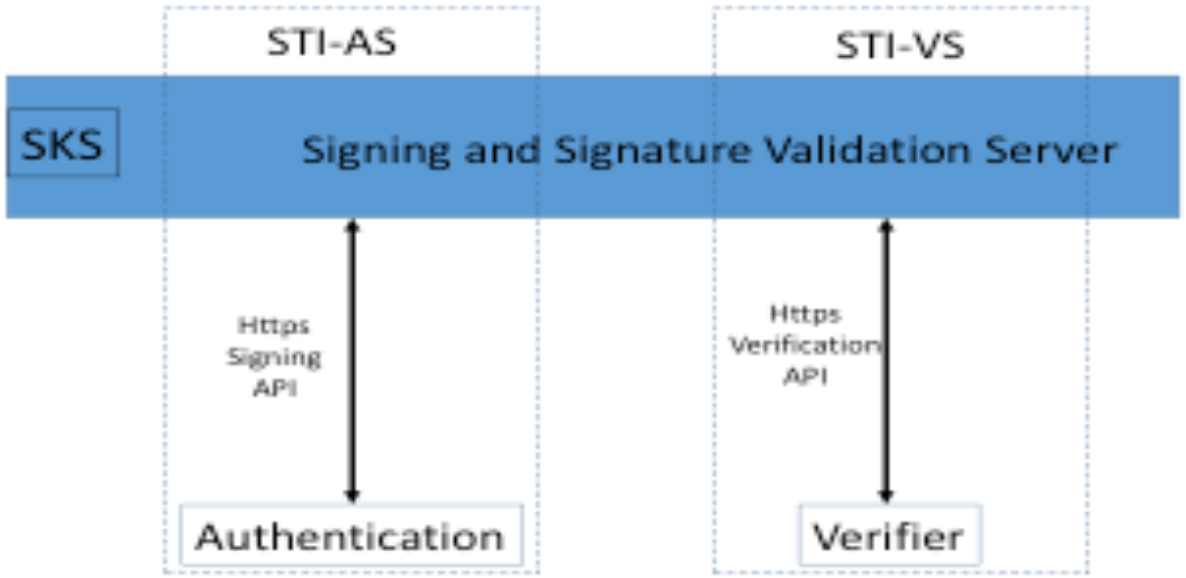
IPNNI Task Group

April 24, 2017

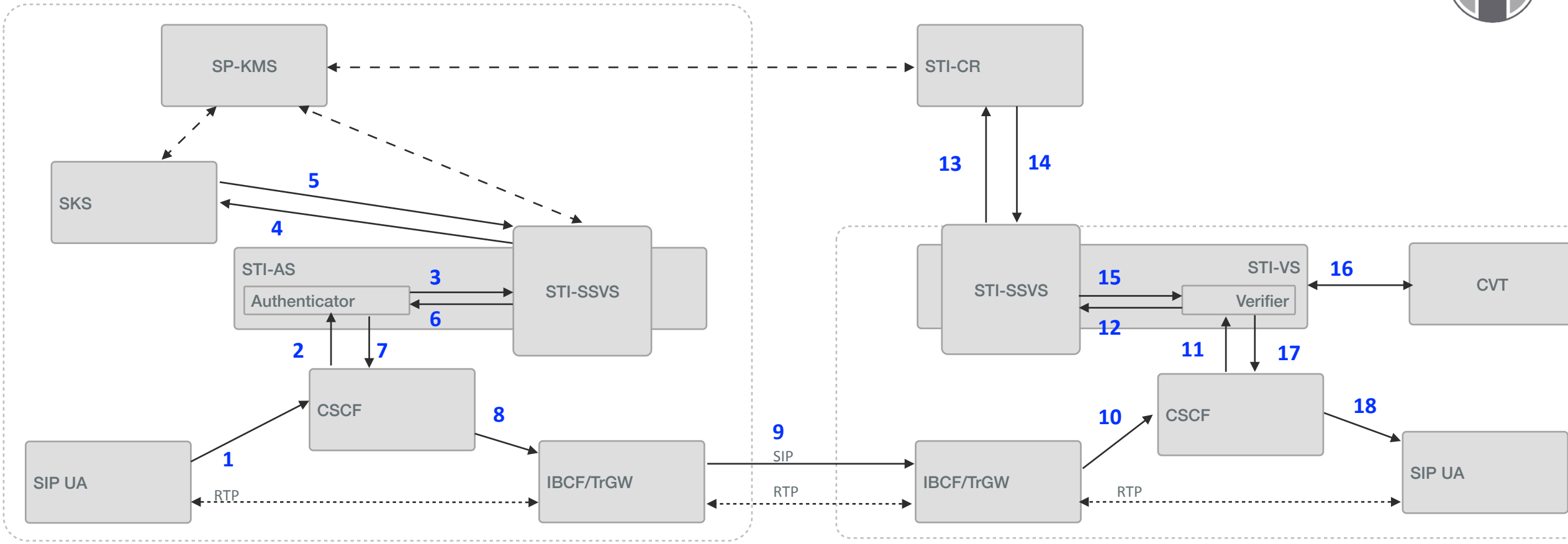
Mary Barnes, iconectiv CTO group

iconectiv

Signing and Signature Validation Server



STI Call Origination & Termination



Service Provider A
Originating/Authorization

Service Provider B
Terminating/Verification

iconectiv

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-SHAKEN Signing and Verification Server (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.

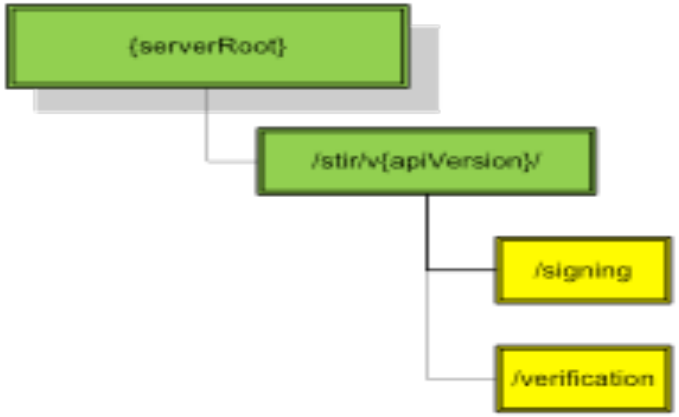
18. The terminating SIP UA receives the INVITE and normal SIP processing of the call continues, returning "200 OK" or optionally setting up media end-to-end.

REST resource structure

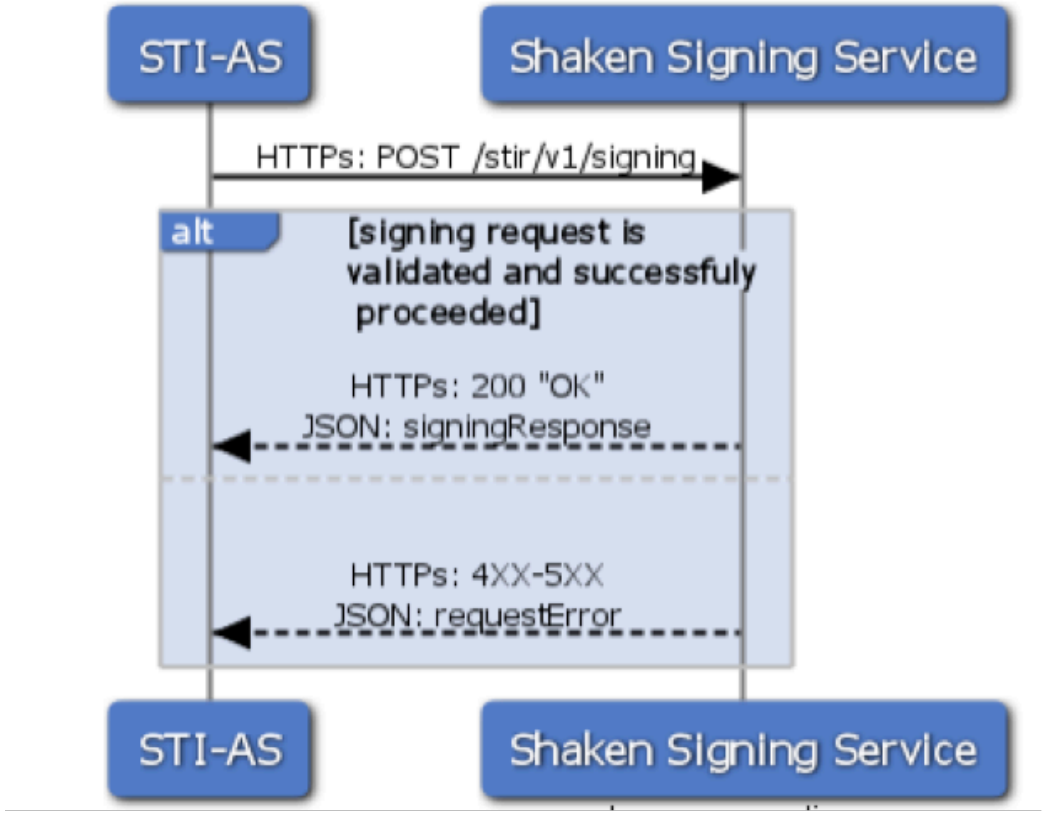
- REST resources are defined with respect to a “server Root” :

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

- The resource structure is provided below:

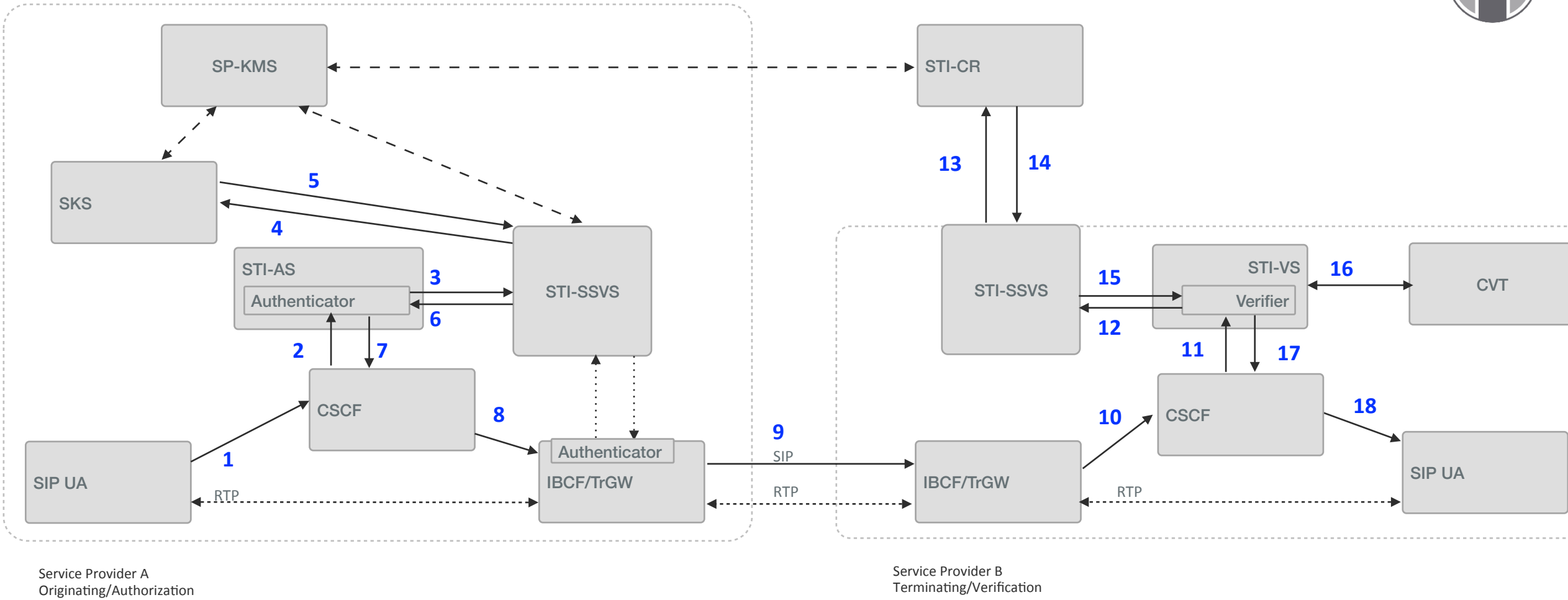


Signing API



- Diagram shows API between STI-AS and Signing Service implying signing service is not in the AS but rather a separate server
- Or should STI-AS label be “Authenticator”?

STI Call Origination & Termination



- Since STI-AS is logical, Authenticator and Verifier can be integral to CSCF
- Contribution IPNNI-2017-0037R00 introduces the notion of the IBCF/TrGW adding Identity header field

iconectiv

Discussion