Request Specification for Server and Application

1. Server

This project needs following 3 types of servers.

3 types of servers are shared to ID and Password used by Digest authentication.

Authentication Server:

[Software construction of this server] WebServer(Apache) + PHP + MySQL

・Scanner and Smartphone's App register Global IP Address and Port Number obtained from STUN/TURN server(HTTP GET Method).

・Scanner and Smartphone's App can acquire Global IP Address and Port Number.

・Prepare a file(*ServerInformation.cfg*) that describes the address and port number of the STUN/TURN server and AudioData server, so as Scanner and Smartphone's App can be obtained(HTTP POST Method).

・authenticate by using ID and Password(same as STUN/TURN Server and Audio Data Server).

・Please publish the address of the Authentication Server to Scanner and Smartphone's App.

STUN/TURN Server:

[Software construction of this server] STUN/TURN Server + MySQL

・more than 2 global IP Addresses.

Scanner accesses to two or more of STUN / TURN server via the NAT, and get the Global IP Address and Port Number. If Global IP Address and Port Number is same, Scanner communicates with Peer2Peer by using the information. If it is different, Scanner is not able to communicate with Peer2Peer because it is a symmetric NAT. Thus, all data are communication by the relay server(TURN Server).

・TURN and STUN server is the same server.

・Server returns Global IP Address for client which has been communicated by STUN protocol.

Audio Data Server(Siren Server):

[Software construction of this server] WebServer(Apache) + PHP + MySQL

・Scanner upload audio data.

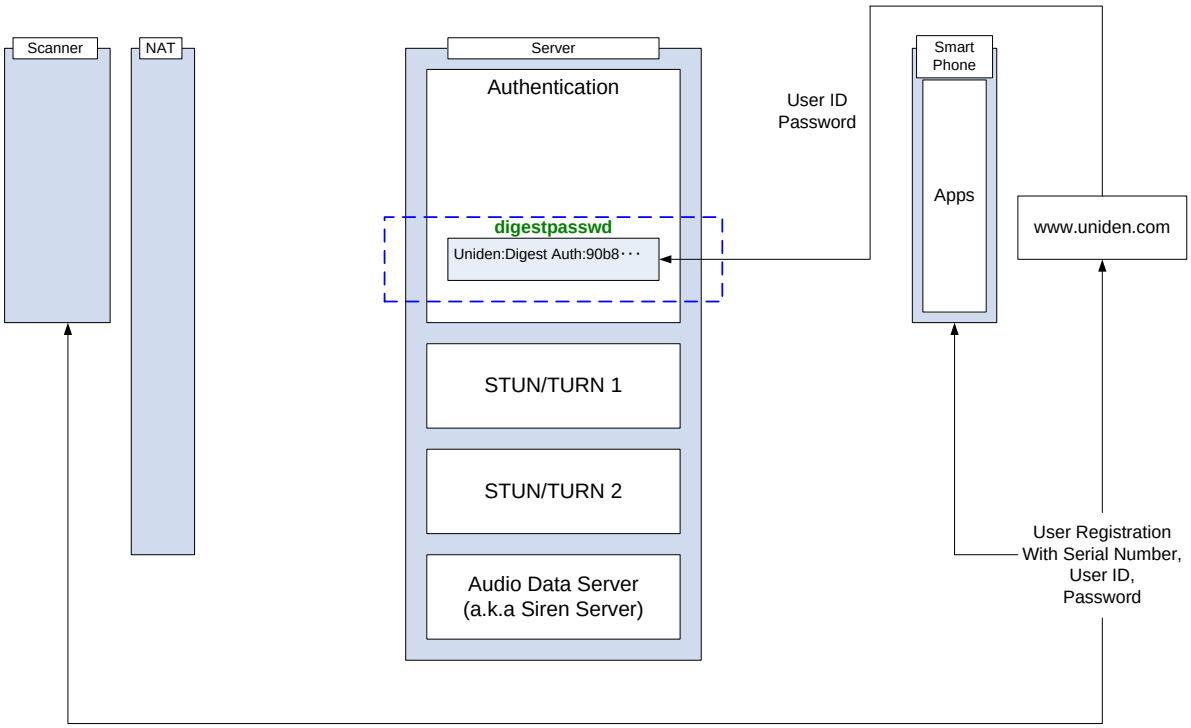
・Smartphone's App download audio data.

・User selectable audio data.

2. Registration User ID and Password

User register Scanner's serial number, User ID and Password in UAC's website.

User ID and Password is determined by the user.



It is registered User ID and Password to the Authentication Server.

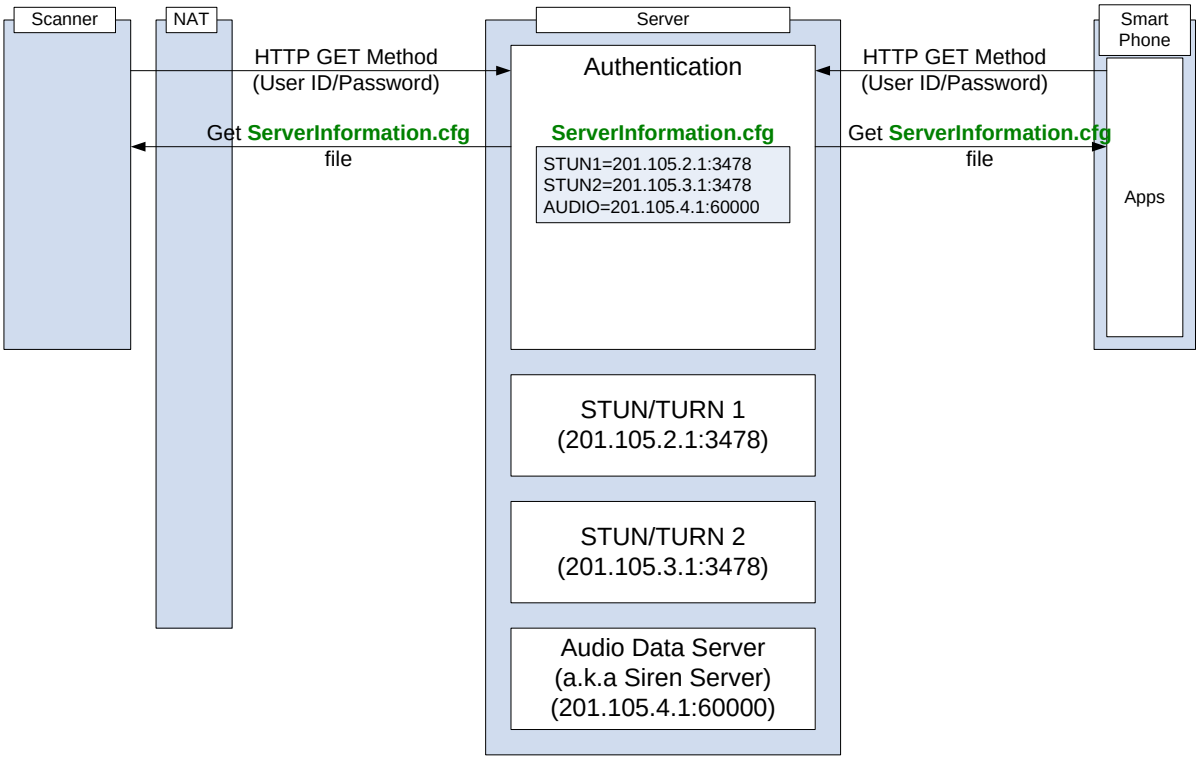
User is registered User ID and Password to be authenticated in UAC's website to Scanner and Smartphone's App.

In addition, User is registered Scanner's serial number in Scanner's menu and Application menu. This is used for file name to be registered in Authentication Server.

3. Acquisition of STUN/TURN Server Address

Authentication Server is stored the address of STUN/TURN Server and Audio Server to ServerInformation.cfg file, it is possible to know the address to retrieve.

ServerInformation.cfg can get by using HTTP GET method and Digest Authentication with registered User ID and Password.



(File Format)

- STUN/TURN1, STUN/TURN2 and Audio Data Server Address + Port Number
- add \n(Line Feed) at the end of line.

STUN1=201.105.2.1:3478\n

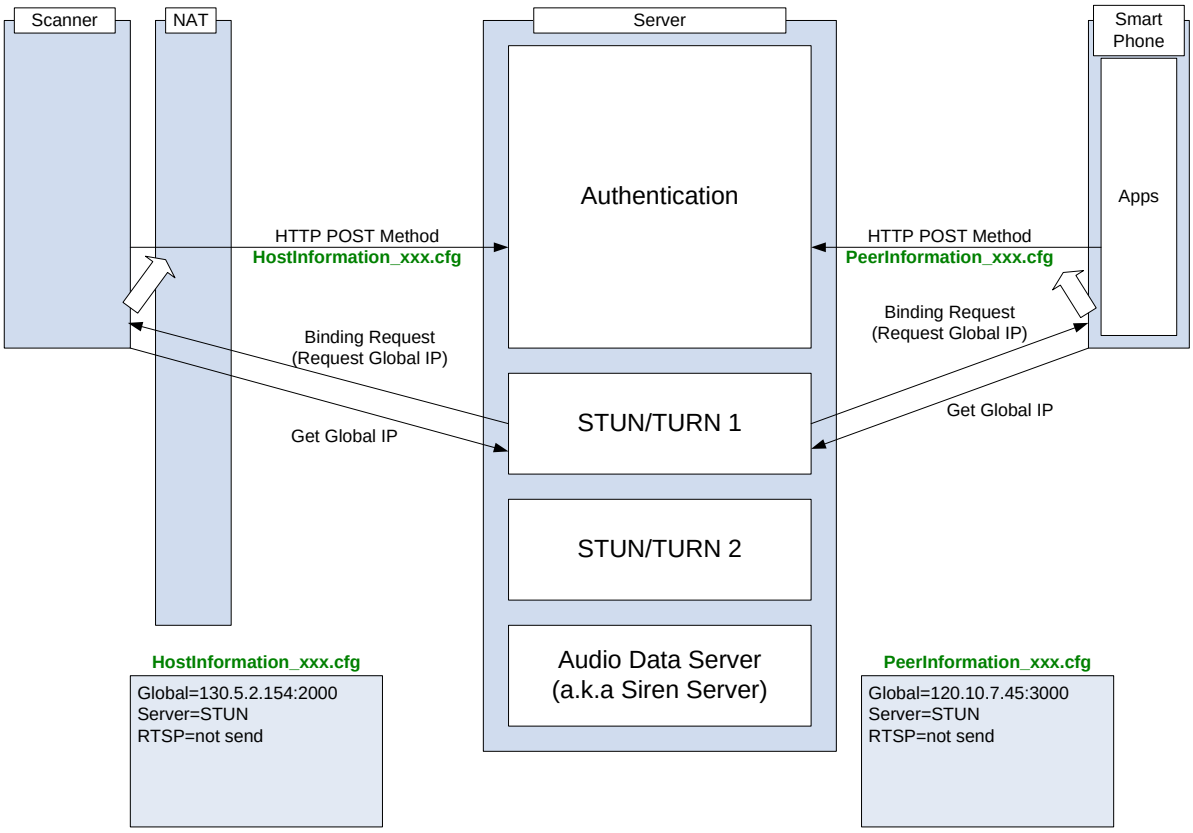
STUN2=201.105.3.1:3478\n

AUDIO=201.105.4.1:60000\n

4. Acquisition of Global IP Address(STUN)

When Client(Scanner or Smartphone's App) send Bind Request of STUN Message(refer to RFC3489 / http://tools.ietf.org/html/rfc3489) in STUN/TURN Server address, Client can acquire its own Global IP Address and Port Number.

Once having acquired the Global IP Address and Port Number, Client transfer the file to Authentication Server by using HTTP POST method.



File Name:

・HostInformation_xxx.cfg : upload Scanner → Authentication

・PeerInformation_xxx.cfg : upload Smartphone's App → Authentication

xxx is Scanner's serial number that User registered in menu.

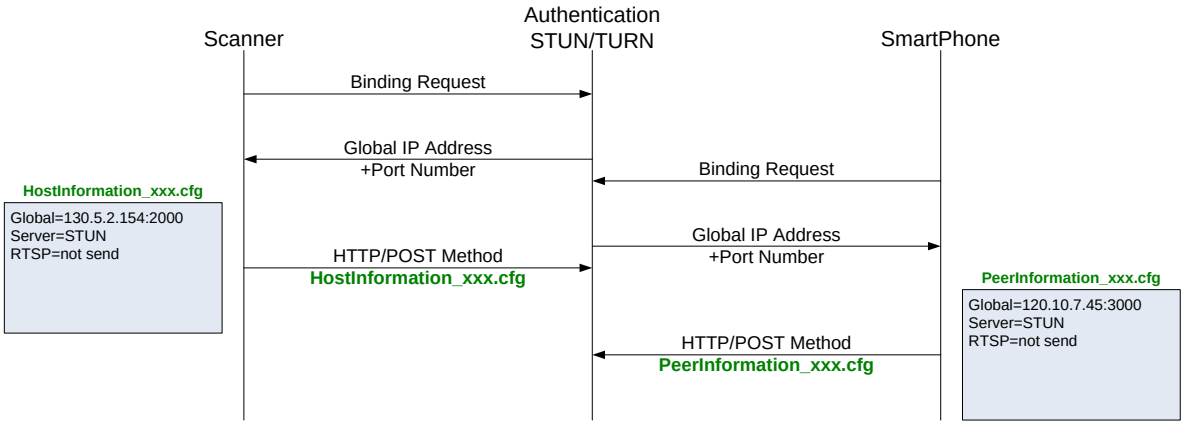
Please publish, if the address to POST file is determined.

(Example) http://xxx.xxx.xxx.xxx/member/upload.php

(File Format)

・Global IP Address, Server ***1*** and the status of RTSP communication.

Global=130.5.2.154:2000\n
Server=STUN or TURN\n
RTSP=not send or sending\n



Scanner will send Binding Request to two or more of the STUN / TURN server with different address.

Scanner write the Global IP Address and Port Number to HostInformation_xxx.cfg file if you can get the same address and port.

If address and port isn't same, since Scanner is connected to a NAT that can't communicate with Peer2Peer (Symmetric NAT), RTSP/RTP communication must relay TURN Server (refer 6. and 7.).

In this case, by sending Allocate Request to STUN/TURN Server, and writes the acquired Global IP Address and Port Number to HostInformation_xxx.cfg.

Please refer RFC2326 / http://tools.ietf.org/html/rfc2326 about RTSP.

1

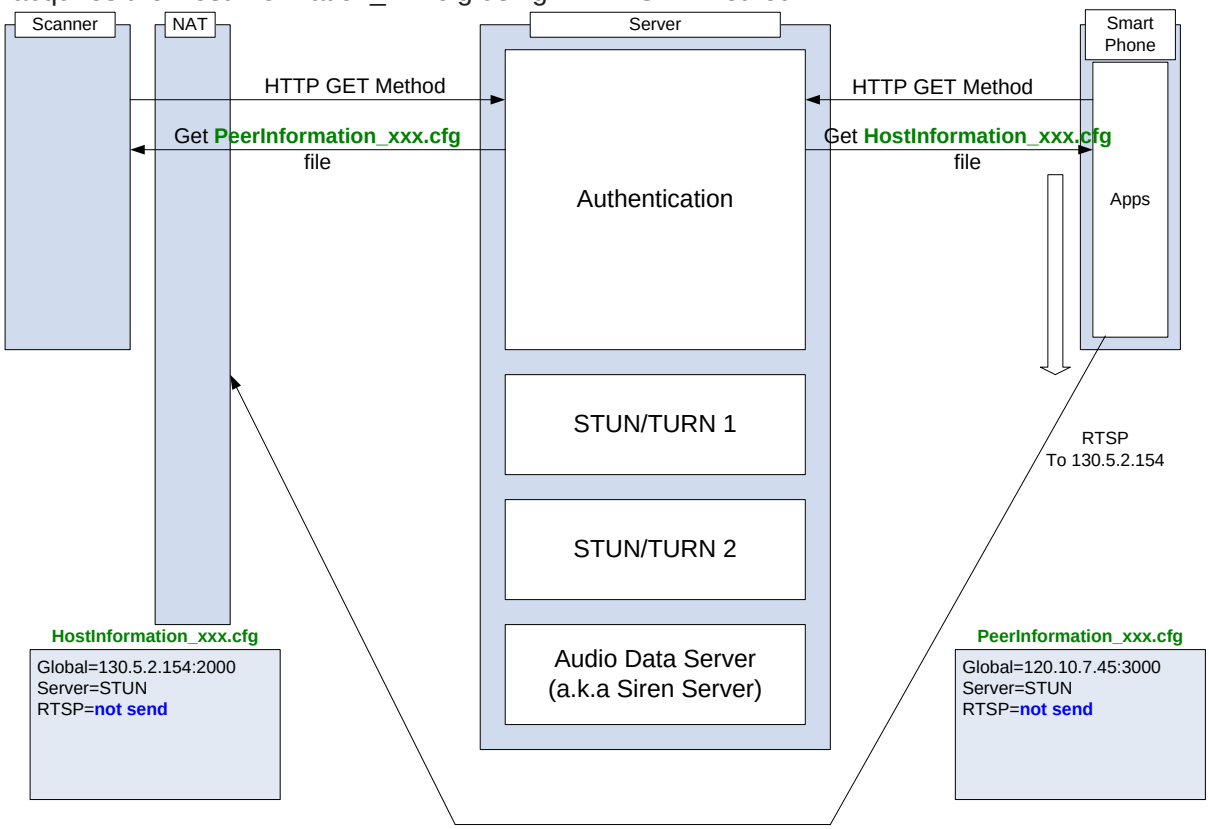
It writes [Server=STUN] if Client acquires Global IP Address by Binding Request, it writes [Server=TURN] if Client acquires Global IP Address by Allocate Request.

When communicating RTSP/RTP relaying TURN Server, Both Scanner and Smartphone's App must use TURN Server.

If Smartphone's App get HostInformation_xxx.cfg and detect the information of [Server=TURN] in HostInformation_xxx.cfg, Smartphone's App switch to the communication to go through TURN Server. In this case, not only RTP, method of RTSP also communicate via TURN Server, all communication is UDP.

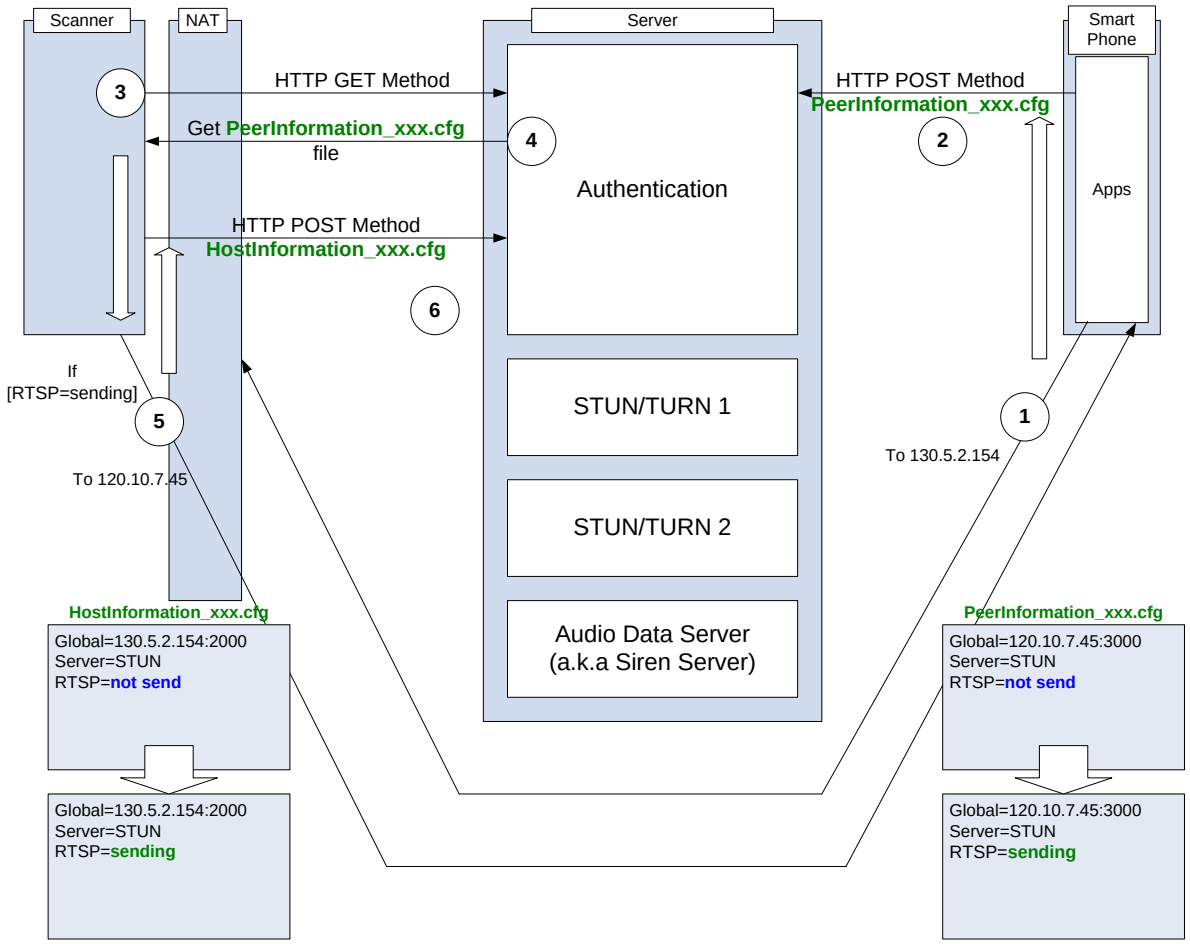
5. RTSP/RTP(Peer2Peer)

In order to know the Global IP Address and Port Number of Scanner, Smartphone's App acquires the HostInformation_xxx.cfg using HTTP GET method.



Smartphone's App start transmitting the RTSP to the Scanner's Global IP Address described in the HostInofrmation_xxx.cfg file.

Next, Smartphone's App updates from [RTSP=not send] to [RTSP=sending] in the PeerInformation_xxx.cfg file, and upload to Authentication Server by using HTTP POST method(②of next figure).



Also, if it is (Port) Restricted cone NAT, Scanner can't receive the RTSP Method from App if Scanner doesn't transmit once for Global IP Address of Smartphone's App.

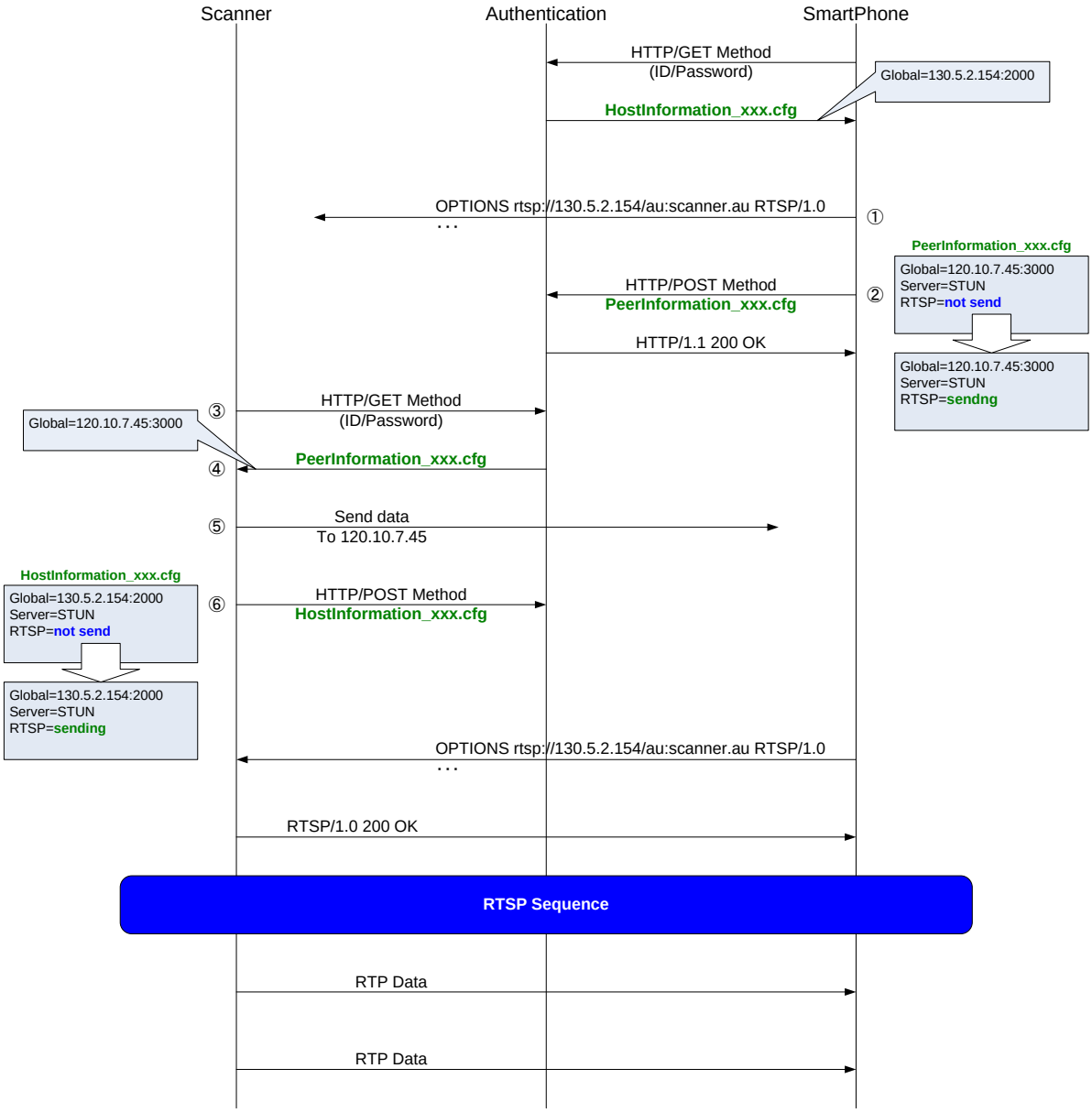
In order to detect that Scanner isn't received although App is sending RTSP, Scanner check the state of [RTSP=] in the PeerInformation_xxx.cfg file regularly (③, ④).

Scanner send data to the Global IP Address and Port Number of Smartphone's App describing in the PeerInformation_xxx.cfg if [RTSP] state is [=sending] and Scanner have not received the RTSP data from Smartphone's App (⑤).

Scanner update from [RTSP=not send] to [RTSP=sending] in the HostInformation_xxx.cfg and upload to Authentication Server (⑥).

Because the results are transmitted to the Smartphone's App from Scanner remains in NAT, next communication is possible (RTSP data transmitted first is discarded).

Sequence between Scanner and Smartphone's App is the follows.



The URL that specify OPTIONS method at the RTSP communication started, it described as follows.

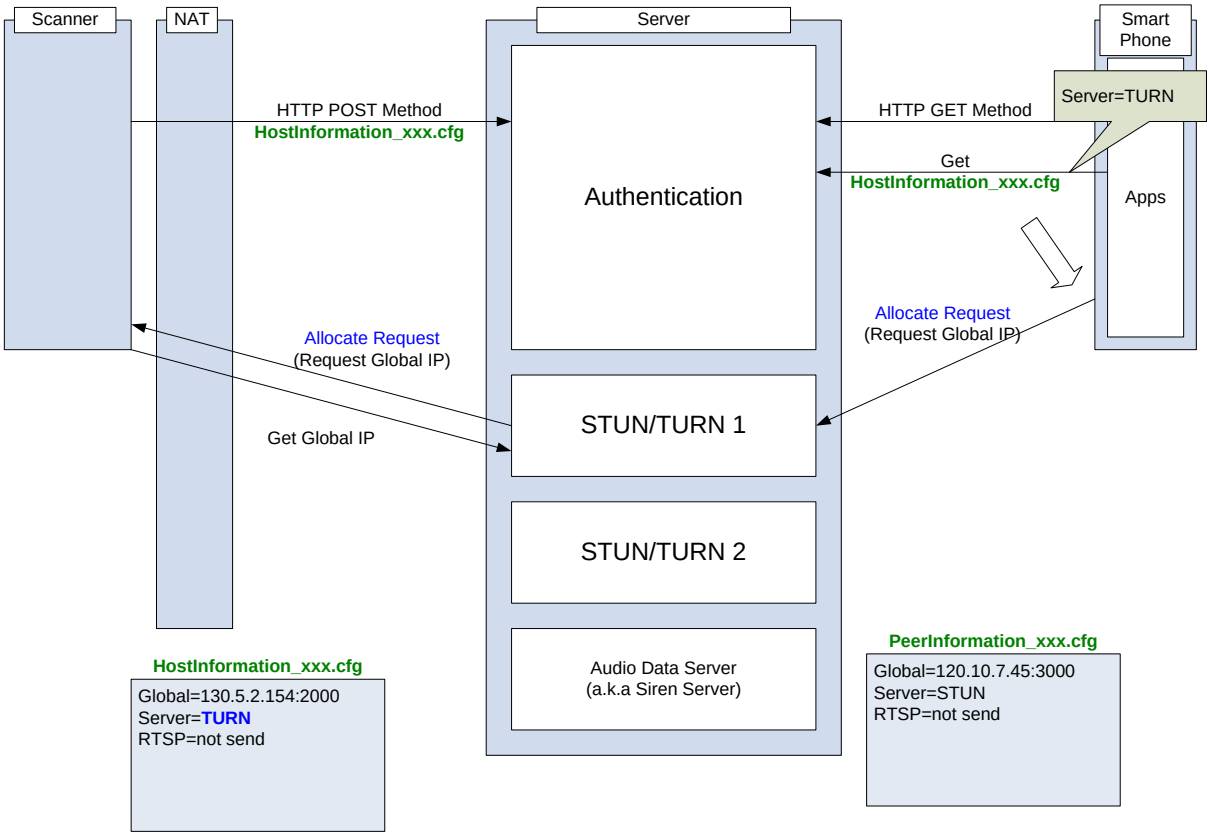
rtsp://xxx.xxx.xxx.xxx/au:scanner.au

xxx.xxx.xxx.xxx is Scanner's Global IP Address.

6. Acquisition of Global IP Address(STUN)

If Global IP Address obtained from two STUN/TURN Server by Binding Request is different, it means that Scanner is connected with the NAT Global IP Address or Port Number is varies by the communication partner.

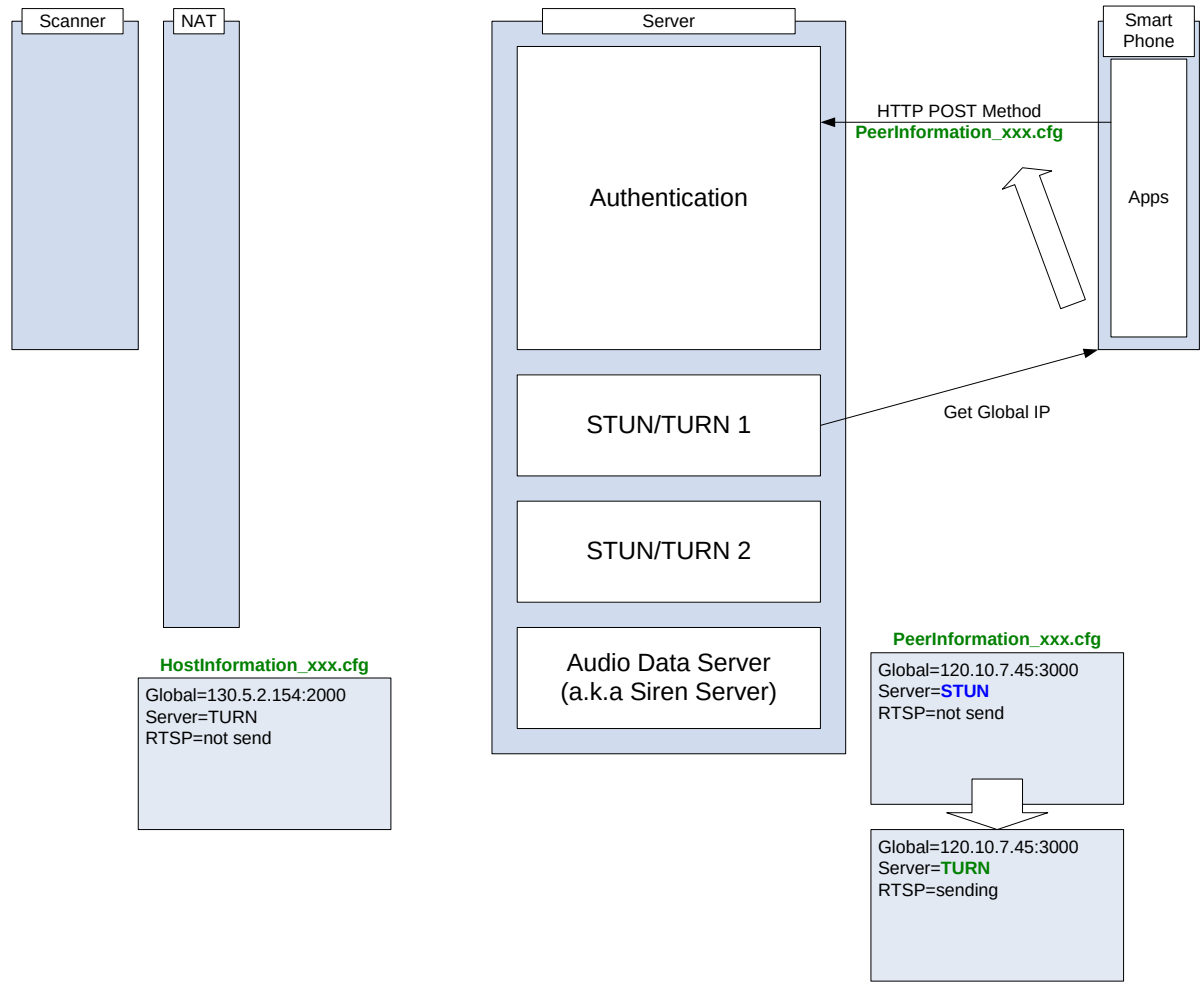
In this case, client must use the STUN/TURN Server as TURN Server.

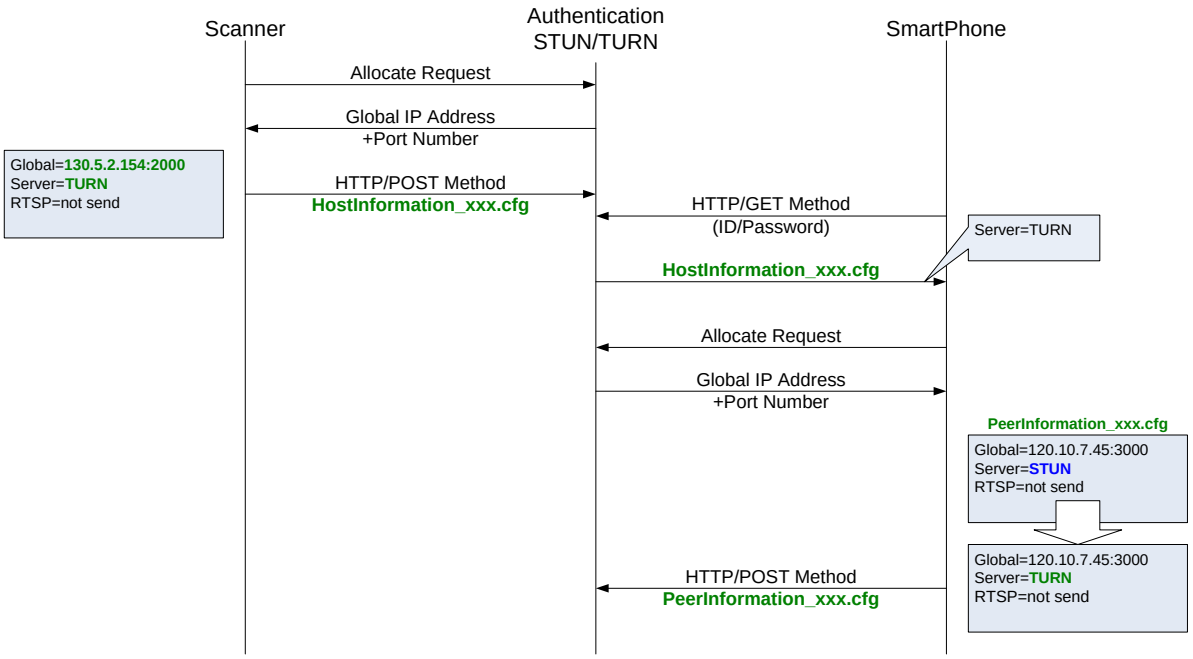


TURN Server return Global IP Address and Port Number when Scanner send Allocate Request (refer to RFC5766 / http://tools.ietf.org/html/rfc5766) to STUN/TURN Server. Scanner describes Global IP Address and Port Number and kind of Server:[Server=TURN], and upload HostInformation_xxx.cfg by using HTTP POST method to Authentication Server. If Scanner is [Server=TURN] and Smartphone's App is [Server=STUN], Smartphone's App switch to TURN Server by the following method.

Smartphone's App downloads HostInformation_xxx.cfg regularly and check [Server=] state of Scanner. If [Server=] state of Scanner is [TURN], Smartphone's App send Allocate Request and acquires Global IP Address and Port Number from STUN/TURN Server.

Next, Smartphone's App update [Global=] and [Server=] (from STUN to TURN), upload PeerInformation_xxx.cfg by using HTTP POST method to Authentication Server.


Scanner
NAT
Server
Smart Phone
Authentication
Apps
HTTP POST Method
PeerInformation_xxx.cfg
STUN/TURN 1
Get Global IP
STUN/TURN 2
Audio Data Server
(a.k.a Siren Server)
HostInformation_xxx.cfg
Global=130.5.2.154:2000
Server=TURN
RTSP=not send
PeerInformation_xxx.cfg
Global=120.10.7.45:3000
Server=STUN
RTSP=not send
Global=120.10.7.45:3000
Server=TURN
RTSP=sending

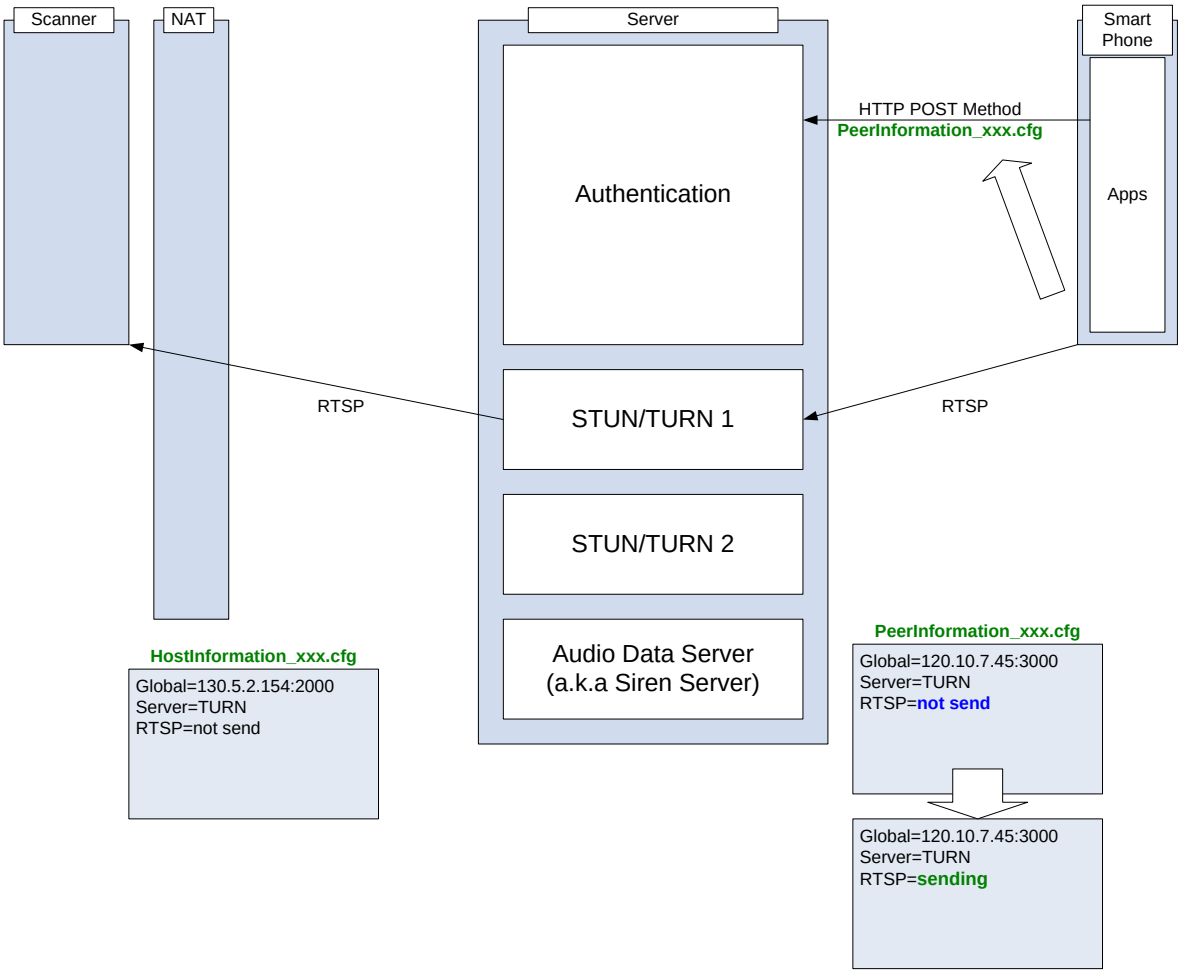

Scanner
Authentication
STUN/TURN
SmartPhone
Allocate Request
Global IP Address
+Port Number
Global=130.5.2.154:2000
Server=TURN
RTSP=not send
HTTP/POST Method
HostInformation_xxx.cfg
HTTP/GET Method
(ID/Password)
Server=TURN
HostInformation_xxx.cfg
Allocate Request
Global IP Address
+Port Number
PeerInformation_xxx.cfg
Global=120.10.7.45:3000
Server=STUN
RTSP=not send
Global=120.10.7.45:3000
Server=TURN
RTSP=not send
HTTP/POST Method
PeerInformation_xxx.cfg

7. RTSP/RTP(relayed TURN)

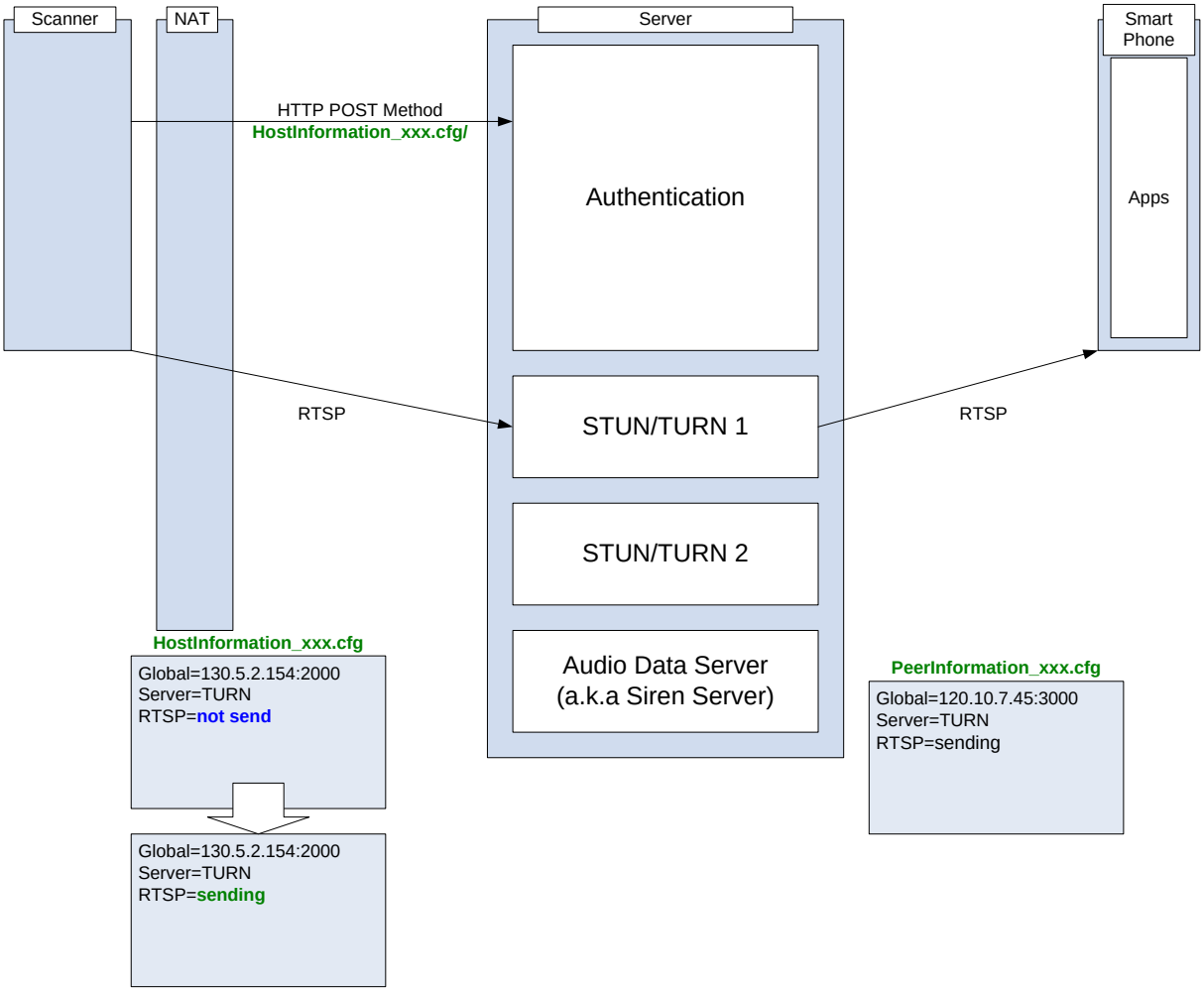
If Scanner and Smartphone's App communicate the RTSP / RTP data relaying TURN server, it is necessary to notify the partner information of the destination (Global IP Address and Port Number) to the TURN server.

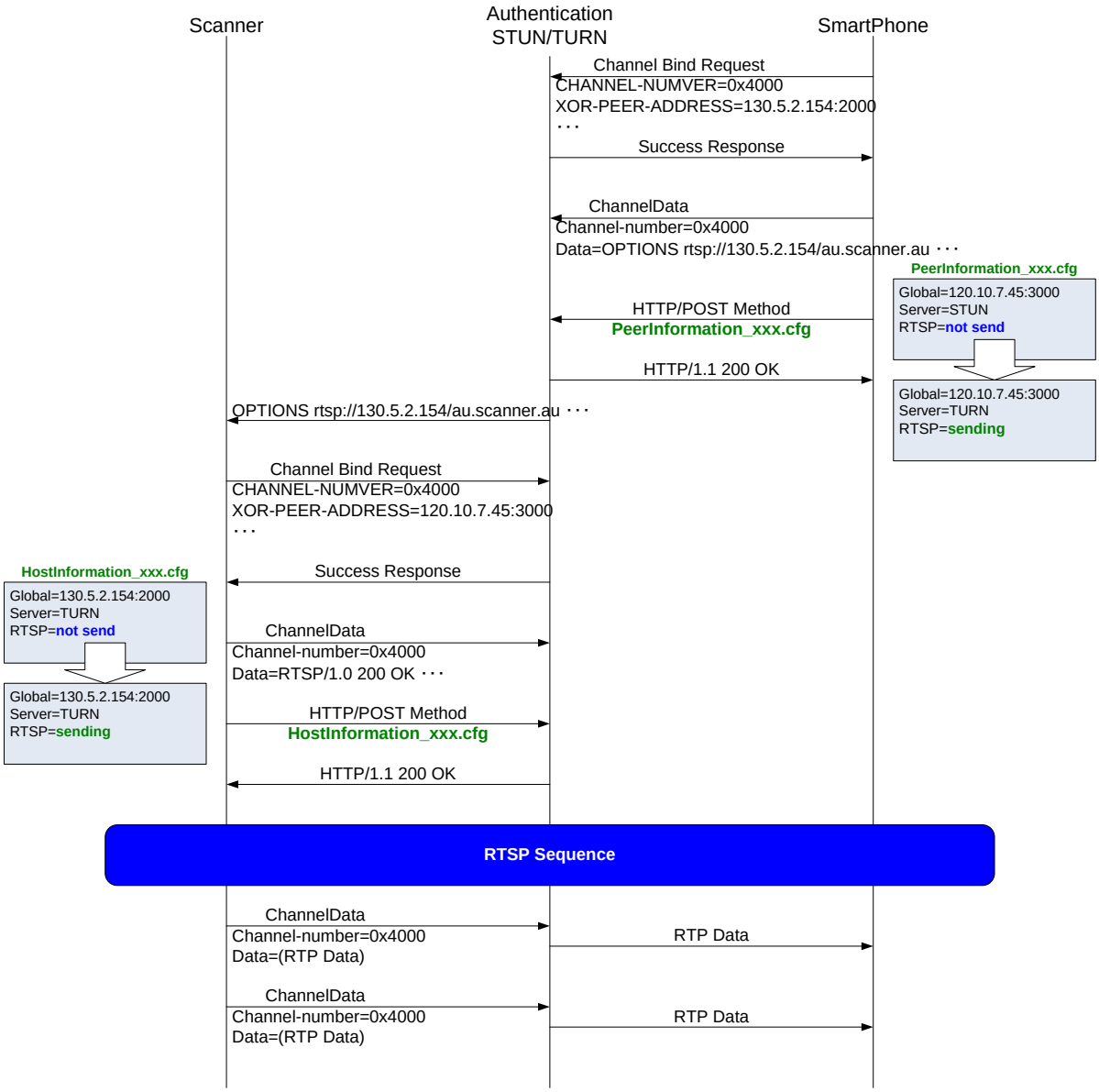
The address of the communication partner are each acquired from HostInformation_xxx.cfg and PeerInformation_xxx.cfg, TURN Server can relay by specifying XOR-PEER-ADDRESS attribute to Channel Bind Request (refer to RFC5766 / http://tools.ietf.org/html/rfc5766).

Once Smartphone's App begin to send RTSP Data to TURN Server, updates to [RTSP=sending], and upload PeerInformation_xxx.cfg by using HTTP POST method to Authentication Server.



If Scanner receives OPTIONS method (RTSP data) from TURN Server, update to [RTSP=sending], and upload HostInformation_xxx.cfg by using HTTP POST method to Authentication Server.


Scanner
NAT
Server
Smart Phone
HTTP POST Method
HostInformation_xxx.cfg/
Authentication
Apps
RTSP
STUN/TURN 1
RTSP
STUN/TURN 2
Audio Data Server
(a.k.a Siren Server)
HostInformation_xxx.cfg
Global=130.5.2.154:2000
Server=TURN
RTSP=not send
Global=130.5.2.154:2000
Server=TURN
RTSP=sending
PeerInformation_xxx.cfg
Global=120.10.7.45:3000
Server=TURN
RTSP=sending


Scanner
Authentication
STUN/TURN
SmartPhone
Channel Bind Request
CHANNEL-NUMVER=0x4000
XOR-PEER-ADDRESS=130.5.2.154:2000
· · ·
Success Response
ChannelData
Channel-number=0x4000
Data=OPTIONS rtsp://130.5.2.154/au.scanner.au · · ·
PeerInformation_xxx.cfg
Global=120.10.7.45:3000
Server=STUN
RTSP=not send
HTTP/POST Method
PeerInformation_xxx.cfg
HTTP/1.1 200 OK
Global=120.10.7.45:3000
Server=TURN
RTSP=sending
OPTIONS rtsp://130.5.2.154/au.scanner.au · · ·
Channel Bind Request
CHANNEL-NUMVER=0x4000
XOR-PEER-ADDRESS=120.10.7.45:3000
· · ·
HostInformation_xxx.cfg
Success Response
Global=130.5.2.154:2000
Server=TURN
RTSP=not send
ChannelData
Channel-number=0x4000
Data=RTSP/1.0 200 OK · · ·
Global=130.5.2.154:2000
Server=TURN
RTSP=sending
HTTP/POST Method
HostInformation_xxx.cfg
HTTP/1.1 200 OK
RTSP Sequence
ChannelData
Channel-number=0x4000
Data=(RTP Data)
RTP Data
ChannelData
Channel-number=0x4000
Data=(RTP Data)
RTP Data