Messaging System

Published 2014-10-28 | (Compatible with SDK 3.5,4.5,5.0,5.1 and 2012,2013,2014 models)

> Description of communication system used by Convergence Framework in Samsung Smart TV. Convergence Framework enables bidirectional communication between TV and different devices such as tablets, smartphones, laptops and desktops.

Contents

The main purpose of the Convergence Framework is to enable transparent two way communication between the TV application and different devices. Each application is responsible for defining its own message formats and interpreting them. A message is XML or JSON text data. Messages can include attachments such as image or audio files.

> Note
>
> Some predefined system messages must be handled by all the applications. All system messages are in JSON format.

The Samsung Smart TV framework creates a message queue for the TV application and a message queue for each client device connected to the application.

The framework supports:

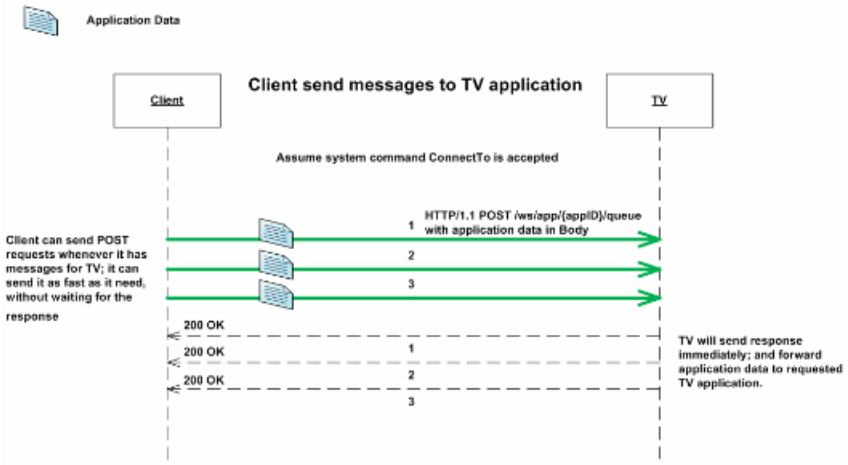
HTTPS for secure communication

The following types of message exchanges:

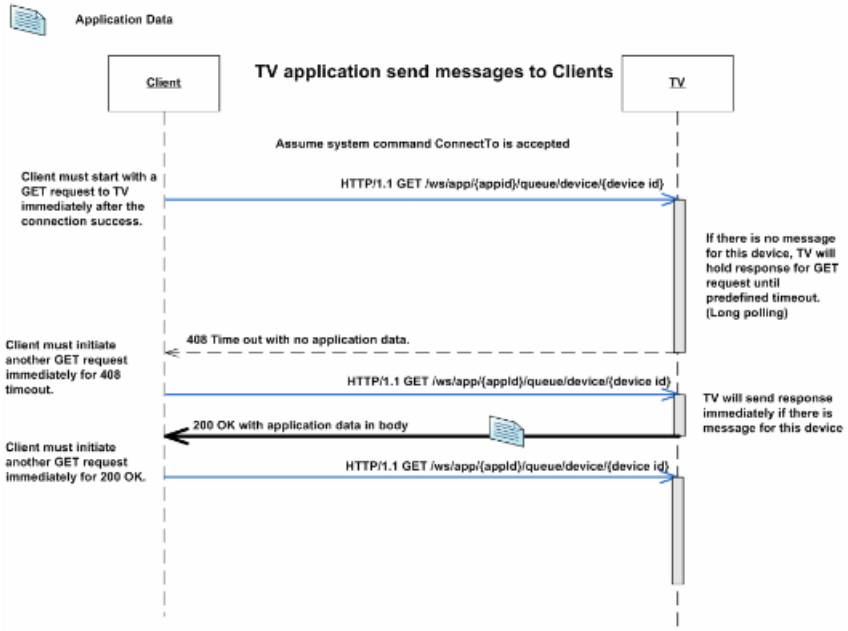
- Device to TV
- TV to device
- TV to device group
- Device to device group

Full-duplex communication in 2 directions:

- Clients to the TV application Clients send messages to the TV application using POST requests.



TV application to clients Once the client device is connected, it must maintain a long polling GET to allow TV applications to send messages to clients at any time.



The Samsung Smart TV framework provides a REST-based interface that allow a client device application to:

- Connect to a TV application.
- Send and receive messages.
- Join or leave a group.
- Retrieve application information.

Security and Authentication

The framework has two stages of security:

1. All Clients must have their MAC address authorized by user, before they can connect to TV.
2. Client can connect to TV using HTTPS for secure communication.

The Samsung Smart TV framework uses the following authentication tools:
Client's MAC address verification
Following the same security rule as wireless remote control: every device/client who wants to connect to the TV must have their MAC address authorized by user (using regular remote control). The first time a user connects their client to their TV, a confirmation window prompts the user to accept/reject the requested MAC address. The client's MAC address and user decision is saved on the local database and it can be changed through Menu->Network->AllShare Settings.
HTTPS Server verification
The TV HTTPS server uses Samsung self-signed server certificates. A client applicaiton wishing to communicate with the TV using HTTPS must request a corresponding CA from Samsung and add it as **Trusted CA** for their HTTPS stack.
HTTPS Client Verification (to be supported in the future)
In future, appplication develolpers will be able to use a Samsung-provided CA (signed by Samsung root CA) to sign their client certificates and to enable client certificates verification in their TV application (config.xml). TV HTTP server will reject

client connections that do not have valid client certificates.

HTTP Requests and Responses

The Convergence Application API is implemented over the standard HTTP protocol.

Request Format

The API calls from the client (smartphone, tablet etc.) to the TV should be in HTTP request format. Each method call uses the following components:

Service end point, including protocol, server, port, and application path
HTTP method to be used for the operation (for example GET/POST)
Path to the resource
Desired response format (for example XML or JSON). Note: only JSON is currently supported.
Message body (optional, only for POST) in application-defined format

Response Format

The Convergence App API supports the following response data formats for HTTP requests:

HTTP Status code
Message body (optional): JSON for system messages, application defined format for application messages

HTTP Status Codes

The Convergence App API uses standard HTTP status codes to indicate the success or failure of API calls. The table below lists the HTTP status code types that can be received in response to a request.

Code	Description
200 OK	Request processed successfully.
201 CREATED	Resource created successfully.
204 NO CONTENT	Request fulfilled but not required to return entity-body.
301 MOVED PERMANENTLY	Requested resource has been assigned a new permanent URI. This usually happens when the TV application is configured using HTTPS, but the client tries to connect over HTTP.
400 BAD REQUEST	Invalid URI, header or parameter.
401 UNAUTHORIZED	Authentication is required to access the resource.
404 NOT FOUND	Requested resource not found.
405 METHOD NOT ALLOWED	Requested method is not allowed for the URI.
408 REQUEST TIMEOUT	Request (long polling) time out. Client needs to re-initiate the request immediately.
409 CONFLICT	This usually happens when the client tries to send multiple long polling GETs for the same device or multiple clients with same device ID try to connect.
413 REQUEST ENTITY TOO LARGE	This usually happens when uploaded file size exceed the limit.
500 INTERNAL SERVER ERROR	Error in the framework internal processing.
503 SERVICE UNAVAILABLE	This usually happens when connected devices reach the maximum limit.

System Limits

The table below lists the limits of the messaging system.

Description	Limit
Maximum number of connected devices	4

Description	Limit
Maximum single uploaded file size	3 MB
Maximum total uploaded files size	3 MB