SPECS Authentication Requirements

There are two main sections of the JSON requests sent from the Alexa service to the SPECS system. The two dealing with Authentication are the session and context sections. Authentication & State reference fields are highlighted below.

- Indicates Authentication & State Fields
- Indicates Depreciated Fields

```
"session": {
    "new": true,
    "sessionId": "amzn1.echo-api.session.[unique-value-here]",
    "application": {
      "applicationId": "amzn1.ask.skill.[unique-value-here]"
    },
    "attributes": {
      "key": "string value"
    },
    "user": {
      "userId": "amzn1.ask.account.[unique-value-here]",
      "accessToken": "Atza|AAAAAAAA...",
      "permissions": {
        "consentToken": "ZZZZZZZ.."
      }
    }
  },

  "context": {
    "System": {
      "device": {
        "deviceId": "string",
        "supportedInterfaces": {
          "AudioPlayer": {}
        }
      },
      "application": {
        "applicationId": "amzn1.ask.skill.[unique-value-here]"
      },
      "user": {
        "userId": "amzn1.ask.account.[unique-value-here]",
        "accessToken": "Atza|AAAAAAAA...",
        "permissions": {
          "consentToken": "ZZZZZZZ.."
        }
      },
      "apiEndpoint": "https://api.amazonalexa.com",
      "apiAccessToken": "AxThk..."
    },
    "AudioPlayer": {
      "playerActivity": "PLAYING",
      "token": "audioplayer-token",
      "offsetInMilliseconds": 0
    }
  },
```

- The HTTP headers received will also require signature verification.

```
POST / HTTP/1.1
Content-Type : application/json;charset=UTF-8
Host : your.application.endpoint
Content-Length :
Accept : application/json
Accept-Charset : utf-8
Signature:
SignatureCertChainUrl: https://s3.amazonaws.com/echo.api/echo-api-cert.pem
```

Amazon requirements for Alexa webserver

- Support HTTP over SSL/TLS
- A valid certificate is held from an **'Amazon-approved certificate authority'**
- Verify signature, certificate URL, and timestamps of HTTPS requests
- Get and verify Application ID for every Alexa request received

Field Definitions

- Session Object – Authentication & State fields
  - **sessionId** (string) – Unique identifier of a user's current session
- Context Object – Authentication & State fields
  - **applicationId** (string) – Represents our skill's application id, unique & provided by amazon. Also contained in the context object.
  - **userId** (string) – Unique identifier, 225 character max., generated on skill enabled on user's account. *Note: re-generates if user disables and re-enables skill.*
  - **accessToken** (string) – OAuth2 token generated by the SPECS server when the ServicePlace Account is linked with the Alexa skill. Used for user authentication to the SPECS system. *Note: field does not appear if null*
  - **apiAccessToken** (string) – token used for accessing Alexa-specific APIs. These permissions will need to be enabled by the user on skill setup. i.e. GET requests to https://api.amazonalexa.com for address data
  - **deviceID** (string) – Unique identifier for the particular Alexa device being used.

Miscellaneous Notes

- The 'session' object is only used in particular requests – Launch, Intent, and End. Depending on the type of request additional session data may be included but all required fields for authentication are also located in the context object.
- The above six fields will allow for authentication and validation of Alexa requests, users, and individual Alexa devices tied to singular/multiple Alexa users.

Basic Proposed Model for POC

This model assumes all needed values are already stored for verification & the Alexa user's ServicePlace account is already linked.

1. Receive Alexa request, verify signature and certificate.
2. Verify Application ID corresponds to our skill's ID.
3. The userId and accessToken are used verify and retrieve particular user's information.
4. The request is then routed to the correct handler, with the user's requested information sent back to the user's Alexa device.