4.5. [illegible](4.5. Extension Grants

4.5. [illegible]

[illegible]URI[illegible]“grant_type”[illegible]

[illegible][OAuth-SAML][illegible]SAML[illegible]2.0[illegible]TLS[illegible]HTTP[illegible]

```
POST /token HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded
grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Asaml2bearer&assertion=PEFzc2VydGlvbiBJc3N1ZUl
```

[illegible]
5.15.2

4.5. Extension Grants

```
   The client uses an extension grant type by specifying the grant type   using an absolute URI
(defined by the authorization server) as the   value of the "grant_type" parameter of the token
endpoint, and by
   adding any additional parameters necessary.
Hardt                          Standards Track                   [Page 42]
```

```
RFC 6749                          OAuth 2.0                   October 2012
   For example, to request an access token using a Security Assertion   Markup Language (SAML)
2.0 assertion grant type as defined by   [OAuth-SAML2], the client could make the following HTTP
request using
   TLS (with extra line breaks for display purposes only):
```

```
     POST /token HTTP/1.1
     Host: server.example.com
     Content-Type: application/x-www-form-urlencoded
     grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Asaml2-
bearer&assertion=PEFzc2VydGlvbiBJc3N1ZUluc3RhbnQ9IjIwMTEtMDU     [...omitted for
brevity...]aG5TdGF0ZW1lbnQ-PC9Bc3NlcnRpb24-
   If the access token request is valid and authorized, the   authorization server issues an
access token and optional refresh   token as described in Section 5.1.  If the request failed
client
   authentication or is invalid, the authorization server returns an
   error response as described in Section 5.2.
```

Revision #1
Created Wed, Mar 25, 2020 11:02 PM by □□□
Updated Wed, Mar 25, 2020 11:03 PM by □□□