Wolfgang Kramer
Torsten Lodderstedt
Hannes Tschofenig
Dick Hardt
Aaron Parecki
Karl McGuinness

Draft-ietf-oauth-v2-1-13
2026-Feb-Mar
Expires: 2026-Sep-2

Digital Trust Protocol Authorization Code Flow

Abstract

This document defines the Digital Trust Protocol Authorization Code flow, which allows third-party clients to access protected resources with Clients on a secure and trusted Digital Trust Network.

1. Introduction

Privacy is one of the most important things to us here and thanks to the growth of online services, we have began to be taken control of our own data. Many services rely on data from untrusted sources, leading to inaccurate or fraudulent data being used in critical processes.

Most online services also require that a third-party access data on behalf of a user, creating such a powerful data around the different service providers rather can allowing these service providers to verify the authenticity of the data, or even worse, the data is being sold to other third-parties.

We need to define a way that will create a trusted network of identity and data providers, which allows allowing services to get verified and trusted information. Taking advantage of the assertion claims provided will allow for more accurate data to be used in critical processes, and reduce fraudulent data.

DTP provides a framework to verify the identity of the first-party requestor and authenticate the request on a built trust and reduced of third-parties. Additionally, the secondary use cases for this mechanism in order to provide a trusted third-party access to protected resources with the user's consent, and verified by DTP.

Further extensions will complement the DTP Authorization Code flow to provide additional use cases.

1.1. Relational conventions

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", and "SHOULD" in this document are to be interpreted as described in "RFC2119 Key words for use in RFCs to Indicate Requirements" [RFC2119]. These keywords are capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations.

1.2. Terminology

"Access Token", "Authorization Code", "Access Token", "Authorization Code", "Authorization Endpoint", "Authorization Grant", "Authorization Server", "Client", "Client Authentication", "Client Identifier", "Client Secret", "Grant Type", "Protected Resource", "Redirection URI", "Refresh Token", "Response Type", and "Token Endpoint" defined by "RFC6749 The OAuth 2.0 Authorization Framework" [RFC6749]. "Access Token Hash", "Authorization Code Hash", "JSONWebToken (JWT)", "JSONWebToken (JWT) Claims Set", "JSONWebToken (JWT) Header", "JSONWebToken (JWT) Payload", "JSONWebToken (JWT) Signature", "JSONWebToken (JWT) Unsecured", "JSONWebKey (JWK)", "JSONWebKey Set (JWKS)", "Key Id (kid)", "Key Type (kty)", "Public Key", "Private Key", "Cryptographic Hash", "Hash", "Hash", "Signature", "Signature", "Signature

The reason for these two claims is to avoid an attacker in control of the clock on the client side to generate a long lived JWT Authentication request.

```
{
   "iss": "3dfd89e1-964b-4ac4-ba46-977fc5f87db9",
   "aud": "https://op.example.com",
   "response_type": "code",
   "client_id": "3dfd89e1-964b-4ac4-ba46-977fc5f87db9",
   "redirect_uri": "https://rp.example.org/cb",
   "scope": "openid",
   "state": "af0ifjsldkj",
   "nonce": "n-0I0_M16U31",
   "claims":
    {
      "id_token":
       {
         "given_name": {"essential": true},
         "family_name": {"essential": true},
         "passport_number": null,
         "nationality": null,
         "birthdate": {"essential": true},
         "place_of_birth": null
       }
    }
}
```

Signing it with the RS512 algorithm results in this Request Object value [JWS]. This value is used in the request Authentication request.

(line wraps within values for display purposes only)


```
eyJhbGciOiJSUzUxMiIsInR5cCI6IkpXVCIsImtpZCI6InJwX2tleV8yIn0.eyJpc3MiOiIzZGZkODllMS05NjRiLTR
YjkiLCJhdWQiOiJoOHRwczovL29wLmV4YWlwbGUuY29tIiwicmVzcG9uc2VfdHlwZSI6InNvZGUiLCJjbGllbnRfaWQ
YzQtYmE0N105NzdmYzVmODdkYjkiLCJyZWRpcmVjdF91cmkiOiJodHRwczovL3JwLmV4YWlwbGUub3JnL2NiIiwic2N
ZSI6ImFoMGlmanNsZGtqIiwibm9uY2UiOiJuLTAxMF9MTZVMzEiLCJjbGFpbXMiOnsiaWRfdG9rZW4iOnsiZ2l1ZWS
On0ydWV9LCJmYW1pbHlfbmFtZSI6eyJlc3NlbnRpYWwiOnRydWV9LCJwYXNzcG9yZF9uZWI1ZXI1On5lbGwsImShdGl
aGRhdGUiOnsiZXNzZW50aWFsIjp0cnVlfSwicGxhY2VfbzZfYmlydGgiOm51bGx9fSwiaWF0IjoxNTY4NzI0OTQ5LCJ
cCI6MTU2ODcyMTAwOSwianRpIjoiYTMyNGM5YRMtYTQ3Y-00MWE4LWFkM2ItMDY5MzIxODE3ZGM5In0.EojFJSr_FgD
LCnwN21e0PFoS1fVYKLwupIfnCduY_1ZiPgVuCM1x9UM5WV9FdogDf-r1BoF-cp9FLCCd8x-C9VIXKHTXO5jkQ-6ji0
```


This JWS can be validated using the Example Keys

9.8. ID token example

The following is a non-normative example of an `id_token` returned by the OP following the specifications as described in Section 2. of [OIDC].

```
{
   "iss": "https://op.example.org/",
   "aud": "3dfd89e1-964b-4ac4-ba46-977fc5f87db9",
   "sub": "142536748",
   "txn": "VlStGX08_Z5jdHi6B-myT",
   "nonce": "n-0I0_M16U31",
   "at_hash":"z0cYnONBc9Tdhg8Udlj3DO6ArL2M-v_70iPj9lnAlnQ",
   "given_name": "Jane",
   "family_name": "Doe",
   "birthdate": "1990-01-30"
}
```

After signing the JWT and add the mandatory claims, we obtain the next [JWS]. (line wraps within values for display purposes only)


```
eyJhbGciOiJSUzUxMiIsInR5cCI6IkpXVCIsImtpZCI6Im9wX2tleV8xIn0.eyJpc3MiOiJodHRwczovL29wLmV4YWl
FJZCI6IjNkZmQ4OWUxLTk2NGItNGFjNC1jYTQ2LTk3NZFjMWY4N2R1OSIsInNlYi16IjE0MjUzNjc0OCIsIm5vbmNlI
VTMkIiwiYXRfaGFzaCI6InowYTlaOTkyZTk2NnoiYlluT05CYzJ1UZGhnUlVkbEozRE8ZQXJMMk8tdI83MGlQajlbkFSbIEiLCJnaXZlbl9
IsImZhbWlseV9uYWl1IjoiRG9lIiwiYmlydGhkYXRlIjoiMTk5MC0wMS0zMCIsImNlcnRpZmllZF9jbGFpbXMiOnsiY
dmVuZXZhbnWiOnsidmFsdWUiOiJkMTUiLXkiLCJmZWFsdWUiOiJkMTUiLXkiLCJmZWFsdWUiOiJkMTUiLXkiLCJ
p7InZhbHVlIjoiR09lIiwiZW50aXRSIjouU2FudGFuZGVyIiwibG9hIjozfSwiY2VydGlmaWVkX2ShdGlvbmFsaXRSI
OnJpdGlzaCIsIm1vdGl0SSI6IlNhbnRhbmRlciIsImvYS16M09sImNlcnRpZmllZF9iaXJ0aGRhdGUiOnsidmFsdWU
SbyxZ4pJqeCvlLXEY52TIWI1SimcjOvl1Cp1zaRgBZaXGoVqHi1kRXkdOSHty6
lZMj3KxoRvTbiaBCH+75U7rif56fR9lgjME57bCGoz7+BBu9YePKtI1KkyHFcMpx
aJc/AKf9xqpHumeqVciUmAsHJrMwIDAQABoAGnMIGkMBGA1UdDgQWBBTs83nk
LtoXFlmBUts3EIxcVvkvcjB1BqNVHSMEbjBsgBTs83nkLtoXFlmBUts3EIxcVvkv
cqFJpEcwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgTClNvbWUtU3RhdGUxITAfBgNV
BAoTGEludGVybmV0IFdpZGdpdHMgUHRlZCBMaTEwb2IIJAMK8/NoyfcazMAwGA1UdEwQF
MAMBAf8wDQYJKoZIhvcNAQEFBQADggEBABw7w/5k4d5dVDgd/OOOmXdaaCIKvt7d
3ntlvISSvAoKT8d81t97On5RrmefBlT3IZyivZpSbfTqe4+vAVkVdLFdWeFpth/F
OZkYUv6A8o5HW0OMQYVX26zIqBcGZQrm3reiSlSBLvp1TWSpCSvYvSkaO4vFpMak
/ICgdZD+rxwxf8Vb/6fntKywMSLgwKhKmJvZ0kRlpqIgIoieiOm1/gpZ35s0Yuor
XZba9ptfLCYSggg/qcd4d0tbHpIKYKwFmf7f5DRGHDSDSSJm+gI7RFE4bQ8q79R
PAfbG1UGuJ0b/oigagcIHhJp851SQRYf3JuNSc17BnK2L5IEtzjqr+Q=
-----END CERTIFICATE-----
```


9.9.2. Private KEY


```
\-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAvtH4wKLYlXZ1fYQFzYtXZVC3fDBXMarzwvb/fHUyJ6NvNStN
+H7GHp3/OhZbSaRyqK5hu5xKtFLgnI0QS6eTlN1Xbczj H45LeMWhFIdcZuHSpzXi
c78kOugMYlvngAJl0F6+T2FNai+01xEIQq9xbwwPYpflViQyJnzGCIZ7VGan6Gb
RKzyTKcB58yx24pJqxCvlLXEY52TIWI15imcjGvLtlCp1za9qBZa4XGoVqHi1kRX
kdDSHty6lZ8Mj3KxoRvTbiaBCH+75U7rif56f09lgjME57bCGoz7+BBu9YePKtI1K
kyHFqMpxaJc/AKf9xqp+UumeqVciUmAsHJrMwIDAQABAoIBAQCYKw0SYSNhXVPk
eHLeM/pXuwR3DkZexPrakOmmMC8b2vIF7mCNNb6hvhVlUp68JCV8SnS2JxAGo8v
1HY+Et3DdwZ3cxnzwh+BEhzgDfoIOmkoGppZPyX/K6kLWtbGUrTtSISOWXbvEXQU
G0gGAvDOzIGTsdMDX7slnU70Ac23JybPYSqBSiE+ky8U4dm2fUHMreOWub4QP5vA/
nqyMqX2FB/MEAbcujakoDQrFCtbmtUY1BbJCKGd9V3cGEqp6HZoH+ahZqrfMc9tgJ
mCHk3YyWZB/bcVXH3CA+s1yavvCOVDBZ3Nw7Pt9zIcv6Rl9UKTy+NxB0jXxR90Hla
Tr8GHISHAoGBAPsD7uXm+BksnGyKYgvlVadBZ8FUFTBbf4B+vboDbx48F0BO/5V
Pra8PC5z8YRSBOQ/WfccPQzakkA28Fz pXlRpXu5JcErVWnyyUiKpX5sw6iPenQR2
JO9hY/GfbK1wUhVHpvMKcX9FqFLSQu2A86jPnFEfFG4BZT4lhTzINKJVZAoGBAMKc
B3YQfVfYYqiBFXzYRdSRLg5cBp/HzuWwXc9vfJ4kQTDKPXe/+nqD67rzeT54uVec
jKoIrsCu4BfEaoyvOT+1KmUfdEpBgYZuuEC4CZf7dgKbXOpPVvZDMyJ/e7HyqTpw
mvIYJLPm2fNAcakn9rNX5mhLwezEIlbplUUeRdraGABAKhZgPYsLkhr2RXevre9R
wkTvdUfD1pbHxtFHqROCjhnhsFCM7JmFcNtdaFqHYczQxiZ7IqxI7jlNsVek2Md
3ggaa5LBKlDmOuP67N9MXUrGSaJSATImBqrBlLf9Vlzktl1VH8LTyHHaRby8fQ8U
i7d3ukaV6HPW09SA3M6iyJ8xAoGAInp4S+3MaTL8SFsj/nfmtcleboaHKc3B1yoP
BMBQyMfNkPbu+PdXTjtvGTknouzkXAX4cwWAec5ppxS8EffEa1sLGxNMxa19vZI
yJaSh2Ik7Ko3ISFT6NrDNKFMCcYMEwgoNKlUDwfktNTnyW/Uk2dgXuMaXSHHN5
XZt59K8CgYArGVOMK7LUmf3dkTIs3tXBm4/IMtUZmWmcP9C8Xe/Dg/IdQhK5CIx4
VX18rgZNeX/5/4nJBQ3LrdLauTIzE20trNRGU6sGMs3x4WQbSq93RRbFzfGIoK74
IOo5yIBxImQO3k5jz3tgF9RJb15SDBIxonuWvOqAERydYvrmEaH0Bxg==
-----END RSA PRIVATE KEY-----
```


10. Acknowledgements

The authors would like to acknowledge James Begg, Roderick Boothby, Desislava Ilieva and Ildefonso Olmedo for their vital support.

11. Normative References

[RFC2616] Fielding, R., "Hypertext Transfer Protocol -- HTTP/1.1", June 1999, <https://tools.ietf.org/html/rfc2616>.

[OAuth.Multiple.Responses] de Medeiros, B., Scurtescu, M., Tarjan, P., and M. B. Jones, "OAuth 2.0 Multiple Response Type Encoding Practices", 25 February 2014, <https://openid.net/specs/oauth-v2-multiple-response-types-1_0.html>.

[OIDC] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, "OpenID Connect Core 1.0 incorporating errata set 1", 8 November 2014, <http://openid.net/specs/openid-connect-core-1_0.html>.

[URN] Moats, R., "Uniform Resource Names", May 1997, <https://tools.ietf.org/html/rfc2141>.

[OAuth.NativeApps] Denniss, W. and J. Bradley, "OAuth 2.0 for Native Apps", October 2017, <https://tools.ietf.org/html/rfc8252>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997, <https://tools.ietf.org/html/rfc2119>.

[JWT] Sakimura, N., Jones, M., and J. Bradley, "JSON Web Token (JWT)", May 2015, <https://tools.ietf.org/html/rfc7519>.

[JWS] Sakimura, N., Jones, M., and J. Bradley, "JSON Web Signature (JWS)", May 2015, <https://tools.ietf.org/html/rfc7515>.

[OAuth.MTLS] Sakimura, N., Lodderstedt, T., Campbell, B., and J. Bradley, "OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens", January 2018, <https://tools.ietf.org/id/draft-ietf-oauth-mtls-07.html>.

[OAuth2.0] Hardt, C., "The OAuth 2.0 Authorization Framework", October 2012, <https://tools.ietf.org/html/rfc6749>.

[OAuth.PAR] Sakimura, N., Lodderstedt, T., Campbell, B., Tonge, D., and F. Skokan, "OAuth 2.0 Pushed Authorization Requests draft-lodderstedt-oauth-par-01", 2 November 2019, <https://tools.ietf.org/html/draft-lodderstedt-oauth-par-01>.

[RFC8417] Hunt, Ed., P., Jones, M., Denniss, W., and M. Ansari, "Security Event Token (SET)", July 2018, <https://www.rfc-editor.org/info/rfc8417>.

Appendix A. IANA Considerations

A.1. Registry Contents

TBD...

- `txn`: review if already exist.
- `errors`: response parameter in PAR.
- `digital_trust_protocol_extension`: for metadata.

Appendix B. Notices

MIT License

Copyright (c) 2020 Grupo Santander

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Appendix C. Document History

[[To be removed from the final specification]]

Authors' Addresses

Alberto Pulido Moyano
Santander
Email: alberto.pulido@santander.co.uk

Victor Herraiz Posada
Santander
Email: victor.herraiz@santander.co.uk

Jorge Oliva Fernandez
Santander
Email: Jorge.OlivaFernandez@santander.co.uk

Davide Bianchini
Santander Technology
Email: davide.bianchini@santander.co.uk