Logdateien von OP und RP mit dynamischer Client-Registrierung ohne optionale Tokenverschlüsselung (Ausschnitte)

RP: Zugriffsversuch auf geschützte Ressource

```
127.0.0.1 - "" [20/Apr/2023:15:59:34 +0200] "GET /valid-user HTTP/1.1" 301 3051 "-" "Mozilla/5.0 (X11; Ubuntu; Linux
x86_64; rv:109.0) Gecko/20100101 Firefox/112.0"
127.0.0.1 - "" [20/Apr/2023:15:59:34 +0200] "GET /valid-user/ HTTP/1.1" 302 947 "-" "Mozilla/5.0 (X11; Ubuntu; Linux
x86_64; rv:109.0) Gecko/20100101 Firefox/112.0"
127.0.0.1 - - [20/Apr/2023:15:59:34 +0200] "GET /discovery.php?target_link_uri=https%3A%2F%2Fsp2.local%2Fvalid-user
%2F&method=get&oidc_callback=https%3A%2F%2Fsp2.local%2Fprotected%2Fcallback&x_csrf=XURuoDz6wNg HTTP/1.1" 200 1059 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0"
```

RP: Ausgehende Konfigurationsabfrage

```
[Thu Apr 20 15:59:41.180517 2023] [auth_openidc:debug] [pid 6817] src/util.c(796): [client 127.0.0.1:47700]
oidc_util_http_call: url=https://idp2.local/.well-known/openid-configuration, data=(null), content_type=(null),
basic_auth=null, bearer_token=(null), ssl_validate_server=1, timeout=5, outgoing_proxy=(null), pass_cookies=0,
ssl_cert=(null), ssl_key=(null), ssl_key_pwd=(null), referer: https://sp2.local/discovery.php?target_link_uri=https%3A%2F
%2Fsp2.local%2Fvalid-user%2F&method=get&oidc_callback=https%3A%2F%2Fsp2.local%2Fprotected%2Fcallback&x_csrf=XURuoDz6wNg
```

OP: Eingehende Abfrage der OP-Konfiguration

```
127.0.0.3 - - [20/Apr/2023:15:59:41 +0200] "GET /.well-known/openid-configuration HTTP/1.1" 303
    3045 "-" "mod_auth_openidc"
127.0.0.3 - - [20/Apr/2023:15:59:41 +0200] "GET /idp/profile/oidc/configuration HTTP/1.1" 200
    2431 "-" "mod_auth_openidc"
```

OP: Antwort mit Konfiguration, Vergabe einer Client ID durch OP

```
==> logs/idp-process.log <==
2023-04-20 15:59:41,349 - 127.0.0.3 - INFO [Shibboleth-Audit.OIDC.Configuration:338] – 127.0.0.3||
    2023-04-20T13:59:41.349289Z|||||||||||||OpenIDConfigurationSuccessResponse|||||mod_auth_openidc
2023-04-20 15:59:41,712 - 127.0.0.3 - INFO [net.shibboleth.idp.plugin.oidc.op.profile.impl.BuildClientInformation:159] -
    Profile Action BuildClientInformation: Client information successfully added to the outbound context
2023-04-20 15:59:41,806 - 127.0.0.3 - INFO [net.shibboleth.oidc.metadata.impl.StorageServiceClientInformationResolver:57]
    - Successfully stored the client information for ID _71f6d421627e10f91b17be9736ccafe9
2023-04-20 15:59:41,808 - 127.0.0.3 - INFO [net.shibboleth.idp.plugin.oidc.op.profile.impl.StoreClientInformation:216] -
    Profile Action  StoreClientInformation: Client information successfully stored for _71f6d421627e10f91b17be9736ccafe9
```

RP: erhält Konfiguration

```
[Thu Apr 20 15:59:41.325186 2023] [auth_openidc:debug] [pid 6817] src/util.c(998): [client 127.0.0.1:47700]
oidc_util_http_call: response={
    "authorization_endpoint":"https:\\/\\/idp2.local\\/idp\\/profile\\/oidc\\/authorize",
    "token_endpoint":"https:\\/\\/idp2.local\\/idp\\/profile\\/oidc\\/token",
    "registration_endpoint":"https:\\/\\/idp2.local\\/idp\\/profile\\/oidc\\/register",
    "issuer":"https:\\/\\/idp2.local",
    "jwks_uri":"https:\\/\\/idp2.local\\/idp\\/profile\\/oidc\\/keyset",
    "scopes_supported":["openid","profile","email"],
    "response_types_supported":["code"],
    "response_modes_supported":["query","fragment","form_post"],
    "grant_types_supported":["authorization_code","implicit","refresh_token"],
    "token_endpoint_auth_methods_supported":["client_secret_basic","client_secret_post","client_secret_jwt",
        "private_key_jwt"],
    "request_object_signing_alg_values_supported":["none","RS256","RS384","RS512","HS256","HS384",
        "HS512","ES256","ES384","ES512"],
    "request_parameter_supported":true,
    "request_uri_parameter_supported":true,
    "subject_types_supported":["public","pairwise"],
    "userinfo_endpoint":"https:\\/\\/idp2.local\\/idp\\/profile\\/oidc\\/userinfo",
    "id_token_signing_alg_values_supported":["RS256","RS384","RS512","ES256","HS256","HS384","HS512"],
    "id_token_encryption_alg_values_supported":["RSA1_5","RSA-OAEP","RSA-OAEP-256","A128KW","A192KW","A256KW",
        "A128GCMKW","A192GCMKW","A256GCMKW"],
    "id_token_encryption_enc_values_supported":["A128CBC-HS256","A192CBC-HS384","A256CBC-HS512",
        "A128GCM","A192GCM","A256GCM"],
    "userinfo_signing_alg_values_supported":["RS256","RS384","RS512","ES256","HS256","HS384","HS512"],
    "userinfo_encryption_alg_values_supported":["RSA1_5","RSA-OAEP","RSA-OAEP-256","A128KW","A192KW","A256KW",
        "A128GCMKW","A192GCMKW","A256GCMKW"],
    "userinfo_encryption_enc_values_supported":["A128CBC-HS256","A192CBC-HS384","A256CBC-HS512",
        "A128GCM","A192GCM","A256GCM"],
    "display_values_supported":["page"],
    "claims_supported":["aud","iss","sub","iat","exp","acr","auth_time","email","email_verified","address","phone",
        "phone_number_verified","name","family_name","given_name","middle_name","nickname","preferred_username",
        "profile","picture","website", "gender","birthdate","zoneinfo","locale","updated_at"],
    "claims_parameter_supported":true},
referer: https://sp2.local/discovery.php?target_link_uri=https%3A%2F%2Fsp2.local%2Fvalid-user
%2F&method=get&oidc_callback=https%3A%2F%2Fsp2.local%2Fprotected%2Fcallback&x_csrf=XURuoDz6wNg
```

RP: speichert sich die OP-Konfiguration

```
[Thu Apr 20 15:59:41.326420 2023] [auth_openidc:debug] [pid 6817] src/util.c(1898): [client 127.0.0.1:47700]
oidc_util_file_write: file "/var/cache/apache2/mod_auth_openidc/sp2.local/idp2.local.provider" written; number of bytes
(2079), referer: https://sp2.local/discovery.php?target_link_uri=https%3A%2F%2Fsp2.local%2Fvalid-user
```

%2F&method=get&oidc_callback=https%3A%2F%2Fsp2.local%2Fprotected%2Fcallback&x_csrf=XURuoDz6wNg

RP: schickt Registrierungsanfrage
[Thu Apr 20 15:59:41.326806 2023] [auth_openidc:debug] [pid 6817] src/util.c(796): [client 127.0.0.1:47700]
oidc_util_http_call: url=https://idp2.local/idp/profile/oidc/register, data={
    "client_name":"sp2.local",
    "redirect_uris":["https://sp2.local/protected/callback"],
    "response_types":["code","id_token","id_token token","code id_token","code token","code id_token token"],
    "grant_types":["authorization_code","implicit","refresh_token"],
    "token_endpoint_auth_method":"client_secret_basic",
    "contacts":["hotline@aai.dfn.de"],
    "jwks_uri":"https://sp2.local/protected/callback?jwks=rsa",
    "id_token_encrypted_response_alg":"RSA1_5",
    "id_token_encrypted_response_enc":"A256GCM",
    "userinfo_encrypted_response_alg":"RSA1_5",
    "userinfo_encrypted_response_enc":"A256GCM",
    "initiate_login_uri":"https://sp2.local/protected/callback",
    "frontchannel_logout_uri":"https://sp2.local/protected/callback?logout=get",
    "backchannel_logout_uri":"https://sp2.local/protected/callback?logout=backchannel",
    "id_token_token_binding_cnf":"tbh",
    "subject_type":"public"},
content_type=application/json, basic_auth=null, bearer_token=(null), ssl_validate_server=1, timeout=5,
outgoing_proxy=(null), pass_cookies=0, ssl_cert=(null), ssl_key=(null), ssl_key_pwd=(null), referer:
https://sp2.local/discovery.php?target_link_uri=https%3A%2F%2Fsp2.local%2Fvalid-user%2F&method=get&oidc_callback=https%3A
%2F%2Fsp2.local%2Fprotected%2Fcallback&x_csrf=XURuoDz6wNg

OP: eingehende Registrierungsanfrage
==> /var/log/apache2/access-idp2.log <==
127.0.0.3 - - [20/Apr/2023:15:59:41 +0200] "POST /idp/profile/oidc/register HTTP/1.1" 201 3599 "-" "mod_auth_openidc"

==> logs/idp-process.log <==
2023-04-20 15:59:41,834 - 127.0.0.3 - INFO [Shibboleth-Audit.OIDC.Registration:338] – 127.0.0.3|
    2023-04-20T13:59:41.421059Z| 2023-04-20T13:59:41.834481Z|||||||||||OIDCClientRegistrationRequest|
    OIDCClientInformationResponse|||||mod_auth_openidc

OP: Datenbankauszug StorageRecords
****
context: oidcClientInformation
     id: _71f6d421627e10f91b17be9736ccafe9
expires: NULL

```
  value: {"grant_types":["refresh_token","authorization_code"],
          "subject_type":"public",
          "application_type":"web",
          "userinfo_encrypted_response_enc":"A256GCM",
          "redirect_uris":["https:\/\/sp2.local\/protected\/callback"],
          "userinfo_encrypted_response_alg":"RSA1_5",
          "token_endpoint_auth_method":"client_secret_basic",
          "client_id":"_71f6d421627e10f91b17be9736ccafe9",
          "id_token_encrypted_response_alg":"RSA1_5",
          "id_token_encrypted_response_enc":"A256GCM",
          "client_secret_expires_at":0,
          "scope":"openid profile email",
          "jwks_uri":"https:\/\/sp2.local\/protected\/callback?jwks=rsa",
          "client_id_issued_at":1681999181,
          "client_secret":"_22b6ca29bc93d0ce7dec55cbb99de18f",
          "client_name":"sp2.local",
          "contacts":["hotline@aai.dfn.de"],
          "response_types":["code"],
          "id_token_signed_response_alg":"RS256"}
version: 1
**************************


OP: eingehender Authentication Request
==> /var/log/apache2/access-idp2.log <==
127.0.0.3 - - [20/Apr/2023:15:59:41 +0200] "GET /idp/profile/oidc/authorize?
    response_type=code
    &scope=openid%20profile%20email
    &client_id=_71f6d421627e10f91b17be9736ccafe9
    &state=NgQY0AxG_sRVLa7hoDjPhSRj1vo
    &redirect_uri=https%3A%2F%2Fsp2.local%2Fprotected%2Fcallback
    &nonce=yO00nscthS_oHoxWvxiGAJtwBjK8NCZgrGTpjUQXn1k
    HTTP/1.1" 302 2757 "https://sp2.local/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0)
    Gecko/20100101 Firefox/112.0"
127.0.0.3 - - [20/Apr/2023:15:59:42 +0200] "GET /idp/profile/oidc/authorize?execution=e1s1 HTTP/1.1" 200 1365
    "https://sp2.local/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0"


==> /var/log/apache2/access-idp2.log <==
127.0.0.3 - - [20/Apr/2023:15:59:43 +0200] "POST /idp/profile/oidc/authorize?execution=e1s1 HTTP/1.1" 302 293
    "https://idp2.local/idp/profile/oidc/authorize?execution=e1s1" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/112.0"
```

```
127.0.0.3 - - [20/Apr/2023:15:59:43 +0200] "GET /idp/profile/oidc/authorize?execution=e1s2 HTTP/1.1" 200 1345
    "https://idp2.local/idp/profile/oidc/authorize?execution=e1s1" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/112.0"
```

OP: Login Endnutzer*in

```
==> logs/idp-process.log <==
2023-04-20 15:59:51,471 - 127.0.0.3 - INFO [net.shibboleth.idp.authn.impl.LDAPCredentialValidator:163] - Credential
    Validator ldap: Login by 'professorin' succeeded
2023-04-20 15:59:51,559 - 127.0.0.3 - INFO [net.shibboleth.idp.authn.impl.FinalizeAuthentication:196] - Profile Action
    FinalizeAuthentication: Principal professorin authenticated


==> /var/log/apache2/access-idp2.log <==
127.0.0.3 - - [20/Apr/2023:15:59:51 +0200] "POST /idp/profile/oidc/authorize?execution=e1s2 HTTP/1.1" 302
    741 "https://idp2.local/idp/profile/oidc/authorize?execution=e1s2" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0)
    Gecko/20100101 Firefox/112.0"
127.0.0.3 - - [20/Apr/2023:15:59:51 +0200] "GET /idp/profile/oidc/authorize?execution=e1s3 HTTP/1.1" 200
    1934 "https://idp2.local/idp/profile/oidc/authorize?execution=e1s2" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
    rv:109.0) Gecko/20100101 Firefox/112.0"
```

OP: User Consent

```
==> logs/idp-process.log <==
2023-04-20 15:59:55,435 - 127.0.0.3 - INFO [Shibboleth-Consent-Audit.OIDC.SSO:338] – 2023-04-20T13:59:55.435218Z|
    _71f6d421627e10f91b17be9736ccafe9
    |AttributeReleaseConsent|professorin|uid,email_verified,mail,displayName,givenName,sn,subject-public
    |vDfwE7BJU6dx2Qifbti7P4cz0SGNyEod4o+ja+27nZo=,DROCrAiyblDGs3TtMi2Q6LU4hCOckZy5E8Yf1HTRJEY=,
    +hOgBHgCbpMxk7iVZ4D6Ghhu5BfRX+1FGqVp9yvxCfA=,80TaoOeYQcUPvXqbuBKxps6kLUd1K3169HbQOp5xzEE=,
    4JdlqOpC26m4kJZR4wrdEQtci+EJbtDs9FdYAWx938g=,mKboPNz1JmHl2z/m/nkTOmdOEu6gTYmZJVYRlzJZ8bE=,
    sM9ascdfGNN1JHtWuapI1JCIpc585xTRQXzgbuBZY58=|true
2023-04-20 15:59:55,542 - 127.0.0.3 - INFO [net.shibboleth.idp.saml.session.impl.SAML2SPSessionCreationStrategy:127] -
    Creating BasicSPSession in the absence of necessary information
```

OP: Authentisierung erfolgreich, generierter Sub Claim für „professorin“ (subject-public) hier sichtbar.

```
2023-04-20 15:59:55,714 - 127.0.0.3 - INFO [Shibboleth-Audit.OIDC.SSO:338] – 127.0.0.3|2023-04-20T13:59:41.985212Z|
    2023-04-20T13:59:55.714248Z |professorin|_71f6d421627e10f91b17be9736ccafe9|||2023-04-20T13:59:51.472380Z||
    5241e5ad778e6a9de03336337da47ddaabf354ecd3deaa0913518eb7647398cb|public|false|||AuthenticationRequest|
    AuthenticationSuccessResponse||||b0a5f2d5584150eb25c536f47b67da693f3bcdd7965d87deafce99dec3b9f6be
    |Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0
```

```
==> /var/log/apache2/access-idp2.log <==
127.0.0.3 - - [20/Apr/2023:15:59:55 +0200] "POST /idp/profile/oidc/authorize?execution=e1s3 HTTP/1.1" 302
    891 "https://idp2.local/idp/profile/oidc/authorize?execution=e1s3" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/112.0"
```

OP: eingehender Access Token / ID Token Request:

```
==> /var/log/apache2/access-idp2.log <==
127.0.0.3 - - [20/Apr/2023:15:59:55 +0200] "POST /idp/profile/oidc/token HTTP/1.1" 200 5495 "-" "mod_auth_openidc"
```

OP: Authentisierung der RP (der Client ID) für Token Endpunkt:

```
==> logs/idp-process.log <==
2023-04-20 15:59:56,063 - 127.0.0.3 – INFO
[net.shibboleth.idp.plugin.oidc.op.authn.impl.OIDCClientInfoCredentialValidator:154] - Credential Validator
    oauth2-clientinfo: Login by '_71f6d421627e10f91b17be9736ccafe9' succeeded
2023-04-20 15:59:56,097 - 127.0.0.3 - INFO [net.shibboleth.idp.authn.impl.FinalizeAuthentication:196] - Profile
    Action FinalizeAuthentication: Principal _71f6d421627e10f91b17be9736ccafe9 authenticated
```

RP:

```
127.0.0.1 - 5241e5ad778e6a9de03336337da47ddaabf354ecd3deaa0913518eb7647398cb [20/Apr/2023:15:59:55 +0200] "GET
/protected/callback?code=AAdzZWNyZXQxD3viPO1t6zI8eY4qzXecG-
y9FhreKNVEv4Ci5lcURUAqIaq8xjfmGhZJqXHrIqJTSLAbR6oCS8DjmspfPuF7AeuBmJqMh9a0sFjdCNwKttSVKY-KRHvzwFv8QlvyFECp5xu9pjB-
T4M32XRAQPDB4JsRI3YGMmIzvLMvUdx4_6RG_itZlja7pTpDrhfw8ZwWpTZR9d-wsos7u-VkpeG0HTryToXR-7m-KyDamEHNHWAS6SII8ljuZsdypxSb-
vgzpFEi1zzD-79lCm28v8fvZtmqlUhSuzS4idFQw8tCszsjjrSuAyCmPZeIpanprR6I_7wLlMt_nFb-7OVgfxrgLxz8BMlYXTLuCFSCy90Amq3Gz-
mLL2VaQgebsGqK2lP5xJHTMFMzQGQdGDsVTii3xpR0eqCnJIybW5zCnhhHN4IRmu5f04HW5p91f5Veer71ZcUivujzqXMYdLM66HbiaWPfRk9XpO_NcODXBfv
ttbFfducGaaa7SJrhVaS-95IgrWMEOaHwLBnJtH-BbwEgOevA3Cku2VVxzof_4YBC&state=NgQY0AxG_sRVLa7hoDjPhSRj1vo HTTP/1.1" 302 1149
"https://idp2.local/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0"
```

OP: verschickt Token Response mit Principal, Sub Claim, Client ID und diversen Standard-Claims

```
==> logs/idp-process.log <==
2023-04-20 15:59:56,555 - 127.0.0.3 - INFO [Shibboleth-Audit.OIDC.Token:338] – 127.0.0.3|2023-04-20T13:59:55.836507Z|
    2023-04-20T13:59:56.536674Z|professorin|_71f6d421627e10f91b17be9736ccafe9|||2023-04-20T13:59:56.094388Z|
    at_hash,sub,aud,auth_time,iss,exp,iat,nonce,sid|5241e5ad778e6a9de03336337da47ddaabf354ecd3deaa0913518eb7647398cb|
    |false|||TokenRequest|OIDCTokenResponse|||||mod_auth_openidc
```

RP: Erhalt von Access Token und ID Token

```
[Thu Apr 20 15:59:56.516132 2023] [auth_openidc:debug] [pid 6819] src/util.c(998): [client 127.0.0.1:44868]
oidc_util_http_call: response={
    "access_token":"AAdzZWNyZXQxkvXCQadeSUt5SjN_-_Gj39qU_29HObF3t3bgGQm_juacszio7EyhW93NqD6517RnlNc54IpNrQ-
V0IgjQekP5Eab8Gkdz0h4I2DJ3oWoOT5B1Ra-aieM4iLek5PdXrEZR_2dSbODSfV2FP3anRanIG4A0M_s5ELY6wjy1_PCRA-
3VIkSNxMZmX2iyfuM06OvL9txz9WQnQokb0JY2aQNNcFVCjwbuSD94Gh5ID0TEiGoKdTiE-_M0bJC1-
```

CTUlnQFREb_mbr5gk1ZIeQSi9JXhX6yngKrW1gpFK0n9QoaK13zTJboejzJJhHohxvuSwByAzB5VyCCeTS0KrOX0XaDby_GhC1pGBeRPfpG_c5twE0yvZbOBP
Oe9LKM-T2pKNBWNSGZ-GHzX-SbB-FEYiw_vAWTKjhio18CCjc7QHV870_erkD9fNo_Vi1qPeT3Sb-8eO8h39WtM4cZ8Ro-
TeoQRAfXg2DHC40kyFY9YlyC_zIEvnGQBwOWlw5Z7_di1b1JUD9sxuOAXPnLw5FsSuT_j_nzqk6Jv20jOu-bssIywBf",
    "scope":"openid profile email",
    "id_token":
"eyJraWQiOiJJMHRRVHZIZ2xJUmRQNXF2RFhKdU9TZU1yeWhwZ1JvN25BOXJuMVhob1FvIiwiY3R5IjoiSldUIiwiZW5jIjoiQTI1NkdDTSIsImFsZyI6IlJT
QTFfNSJ9.b50kHITbYy2vr2r51fHoNvKd-6SCWIn-QyClIR6HRIt2Es_zzBHk3LjNq-POM0O7DwKVoHkTKHSNUN60llySpOarZHHdDgB5y-
lfeDa5oAI5d29DXzysdVC1sgGNCsOk6Woj1izubxMeyrIvYXuoFEPfgXeoBYcArYDDTLV70dDKYWQVONyp71oBh_2ODOnbRH2EHkKdUgf9FPYl6JKt5v28QDW
ljEJ735DXP2a8qUu60UhJVgDXDoJ4U492tRZABjUgVNYGv7fm3N7FLtkxymgztkwQLwWB18DOqPQGq10B2oM0vQ038BRBzWac4mdVg6s3bQ-
QwqmI7DVe2xMSaj7-HYa8pclEp2ZSmIx08xKg9XdRQNDRrF6NKz2-ZOqEKRS5nzjv2lTfVLcfRq6hpxaQuK5jeSjLTNS-
lZKf8PXeepM_X8rUggkfI3_gYnwGpkVRKvVt3xV-uuK2qQ4QJWZUqAWTV2VTmvuANpQleXjRfVBnPKz9wd1oX0v0Xi4eBeXpmKOZZFUrnCb7azzj1-
F9tcGdu9bGuN6dNVRsQxhlArH4kOPhzUeYhcgzyyeoalgj9s-c4jafWRZ-
UnrejkgiUoxMQz8AxxZzqaHji1mSjr69Ha4RQCrc3hZqmUr4vy5VzTIBP3WUcKIjyzJ6-
M9XPaIfLoQsoCIljorRy0s.d3eU_CXo7VbVpbEW.QrBSsXH8ueEptdh9Lgaudfc2JSETA6ilZOSlvqCeRVlC6dO4aVmVJTph5bX3gbu5ghRpG8263MO8ONRnl
5yncxPdXZPO9KE48EMVwvT0ZvvCXtzk0i6F2weNE0mv_nyC7l4ND0-
1ODYPAPAMkQQLSJjNh1nV4xr2LpNcVeeX9aWhLGoDa_8SlEnlgGv3eWVxFrOUF4s85I5csnZDmWQ87zNtLujmfnw-_SHshUnAlguRITjE2-
HjEzc1fg2IxMOsbzOlf8GZdf7dj7wkUcPy07sOyACegFiMvGVYb0RA6x6ObkcEyeZ2Lq6hqq4YHPe6aJL8B8KmDVabrh6jUJoYhqr5ST_gNBIc91rrwTQeNvR
0jbDQczY_EXGQSVqEq4SgYB4NZ89vzGDX1q3k3kHnBlju8NFQji_Na3iJPtmiU31uuO_vvhbJ9ltgCf2QIcftia1QwqCbCDvBPcmYqAV2XNzclLOv1mBoj-
NM3UDDmpF7fEBd2plGR74WnCvA9TEWHQQsxlitqomU0v37YE_emvP6c7gzhTWJ3dw9EJR-
3O27aAKCgRIcAv_ql489wBGRXI47pZ2AISdIuxtSQzygbp8_4w7-6Sn0gCPRKSwt6ZfNQxO8vNP2nKIME61eTjzeI6YWiLSsxpUnwA_i_9T-Psd-
mtRsUeZoUlumjvAYLUCvlSX9u9eEVuqO4KMHu9S3ylc5e-q7yF3GOkx3RioNAzgaXJQv-
xDkLrKr41tfTj_JpWTnLcnpjiaN2k5ZFCklRSWSY0BobChnbNrP8Y9nxAhs_7wVmsAOj6AerL43qpNMLwFUxozRTW7bj9T6Rdd7jkqqcV-
lMPCyNVt78sq_cg6ldxJtjchPHdQW7VCNu5eG2WOZOKjDQSVv-
AvpqAUi9Z9lb2oRxCnoKmYAqIZ4G6XNRm15BxKGgB03TkpG5IvUbBPoHcakqfQUnHoWnFDns9Q6zKfxr6wJKCpd9uEH65VH47gTvafzMrHwLc0gpRtPciyl-
GmGMlgvFhWYLE1xfIc6G3y3buhHAezidIPUCRW48K60D_1yABtaztN2zSFPawl42FtIOQdYLuZnGPI1j8tWbpTcpsRxyeliFaMP9Qu7XNsEHEE.Z4V-
eUxbjn4N1YgETtrMfw",
    "token_type":"Bearer",
    "expires_in":600}, referer: https://idp2.local/

RP: Auslesen des JWT

[Thu Apr 20 15:59:56.632218 2023] [auth_openidc:debug] [pid 6819] src/proto.c(1659): [client 127.0.0.1:44868]
oidc_proto_parse_idtoken: successfully parsed (and possibly decrypted) JWT with
    header={"kid":"defaultRSASign","alg":"RS256"}, and
    payload={
    "at_hash":"mSGiXlf3yodv4X3On3gF8Q",
    "sub":"5241e5ad778e6a9de03336337da47ddaabf354ecd3deaa0913518eb7647398cb",
    "aud":"_71f6d421627e10f91b17be9736ccafe9",
    "auth_time":1681999191,
    "iss":"https:\\/\\/idp2.local",
    "exp":1682002796,
    "iat":1681999196,
    "nonce":"yO00nscthS_oHoxWvxiGAJtwBjK8NCZgrGTpjUQXn1k",

```
    "sid":"_a7ccdf74d25c45fd0bd979a70788e9e0"},
referer: https://idp2.local/
[Thu Apr 20 15:59:56.793471 2023] [auth_openidc:debug] [pid 6819] src/proto.c(1400): [client 127.0.0.1:44868]
oidc_proto_get_key_from_jwks: search for kid "defaultRSASign" or thumbprint x5t "(null)", referer: https://idp2.local/
```

OP: eingehende Abfrage des Schlüsselmaterials für Signaturvalidierung:

```
==> /var/log/apache2/access-idp2.log <==
127.0.0.3 - - [20/Apr/2023:15:59:56 +0200] "GET /idp/profile/oidc/keyset HTTP/1.1" 200 3785 "-" "mod_auth_openidc"
```

OP: Zurückgeben des Keyset

```
==> logs/idp-process.log <==
2023-04-20 15:59:56,821 - 127.0.0.3 - INFO [Shibboleth-Audit.OIDC.Keyset:338] – 127.0.0.3||
 2023-04-20T13:59:56.804793Z|||||||||||||KeySetSuccessResponse|||||mod_auth_openidc
```

RP: Signaturvalidierung

```
[Thu Apr 20 15:59:56.793598 2023] [auth_openidc:debug] [pid 6819] src/proto.c(1462): [client 127.0.0.1:44868]
oidc_proto_get_key_from_jwks: found matching kid: "defaultRSASign" for jwk: {
    "kty":"RSA",
    "kid":"defaultRSASign",
    "e":"AQAB",
    "n":"g-k573Ex1LoHkFokWa-
iBtuWppZ2ghnFdMUNLtHYB7QIiGL2hLyN9IM73cG1DKATWVQS8Mx88LQDYY5iVU1oLCqhDvJiDGT4ij52U8CFP2AjmUuDU8E0upvqf_leq8tS2fR-
RYI0zT42fHVkKrOyX0cn91ZH86CSL6RfoarMlm6u8jL8FN2KBg_VAgbq91JmWpIhcyHzYcBrlXlk6puvM68mVh9RdigvsNtC1NfZszt-
rtENxRq0viLhgLXanZjmQVaH6uqDYzgwzj6DNAzTT2dfZvu1KNltgz-8tSckJr8KNWAG-jfJH36kxHNFFOOzzIzkLPH-Ez6a5Qc47m2RXw"
}, referer: https://idp2.local/
[Thu Apr 20 15:59:56.793700 2023] [auth_openidc:debug] [pid 6819] src/proto.c(1588): [client 127.0.0.1:44868]
oidc_proto_jwt_verify: JWT signature verification with algorithm "RS256" was successful, referer: https://idp2.local/
[Thu Apr 20 15:59:56.793709 2023] [auth_openidc:debug] [pid 6819] src/proto.c(1354): [client 127.0.0.1:44868]
oidc_proto_validate_idtoken: enter,
    jwt.header="{
        "kid":"defaultRSASign",
        "alg":"RS256"}",
    jwt.payload="{
        "at_hash":"mSGiXlf3yodv4X3On3gF8Q",
        "sub":"5241e5ad778e6a9de03336337da47ddaabf354ecd3deaa0913518eb7647398cb",
        "aud":"_71f6d421627e10f91b17be9736ccafe9",
        "auth_time":1681999191,
        "iss":"https:\\/\\/idp2.local",
        "exp":1682002796,
        "iat":1681999196,
```

```
        "nonce":"yO00nscthS_oHoxWvxiGAJtwBjK8NCZgrGTpjUQXn1k",
        "sid":"_a7ccdf74d25c45fd0bd979a70788e9e0"}",
    nonce="yO00nscthS_oHoxWvxiGAJtwBjK8NCZgrGTpjUQXn1k", referer: https://idp2.local/
```

RP startet UserInfo-Abfrage:

```
[Thu Apr 20 15:59:56.793816 2023] [auth_openidc:debug] [pid 6819] src/mod_auth_openidc.c(1133): [client 127.0.0.1:44868]
oidc_retrieve_claims_from_userinfo_endpoint: enter, referer: https://idp2.local/

[Thu Apr 20 15:59:56.793833 2023] [auth_openidc:debug] [pid 6819] src/proto.c(2308): [client 127.0.0.1:44868]
oidc_proto_resolve_userinfo: enter, endpoint=https://idp2.local/idp/profile/oidc/userinfo,
access_token=AAdzZWNyZXQxkvXCQadeSUt5SjN_-_Gj39qU_29HObF3t3bgGQm_juacszio7EyhW93NqD6517RnlNc54IpNrQ-
V0IgjQekP5Eab8Gkdz0h4I2DJ3oWoOT5B1Ra-aieM4iLek5PdXrEZR_2dSbODSfV2FP3anRanIG4A0M_s5ELY6wjy1_PCRA-
3VIkSNxMZmX2iyfuM06OvL9txz9WQnQokb0JY2aQNNcFVCjwbuSD94Gh5ID0TEiGoKdTiE-_M0bJC1-
CTUlnQFREb_mbr5gk1ZIeQSi9JXhX6yngKrW1gpFK0n9QoaK13zTJboejzJJhHohxvuSwByAzB5VyCCeTS0KrOX0XaDby_GhC1pGBeRPfpG_c5twE0yvZbOBP
Oe9LKM-T2pKNBWNSGZ-GHzX-SbB-FEYiw_vAWTKjhio18CCjc7QHV870_erkD9fNo_Vi1qPeT3Sb-8eO8h39WtM4cZ8Ro-
TeoQRAfXg2DHC40kyFY9YlyC_zIEvnGQBwOWlw5Z7_di1b1JUD9sxuOAXPnLw5FsSuT_j_nzqk6Jv20jOu-bssIywBf, referer: https://idp2.local/

[Thu Apr 20 15:59:56.793845 2023] [auth_openidc:debug] [pid 6819] src/util.c(796): [client 127.0.0.1:44868]
oidc_util_http_call:
    url=https://idp2.local/idp/profile/oidc/userinfo,
    data=(null),
    content_type=(null),
    basic_auth=null,
    bearer_token=AAdzZWNyZXQxkvXCQadeSUt5SjN_-_Gj39qU_29HObF3t3bgGQm_juacszio7EyhW93NqD6517RnlNc54IpNrQ-
V0IgjQekP5Eab8Gkdz0h4I2DJ3oWoOT5B1Ra-aieM4iLek5PdXrEZR_2dSbODSfV2FP3anRanIG4A0M_s5ELY6wjy1_PCRA-
3VIkSNxMZmX2iyfuM06OvL9txz9WQnQokb0JY2aQNNcFVCjwbuSD94Gh5ID0TEiGoKdTiE-_M0bJC1-
CTUlnQFREb_mbr5gk1ZIeQSi9JXhX6yngKrW1gpFK0n9QoaK13zTJboejzJJhHohxvuSwByAzB5VyCCeTS0KrOX0XaDby_GhC1pGBeRPfpG_c5twE0yvZbOBP
Oe9LKM-T2pKNBWNSGZ-GhzX-SbB-FEYiw_vAWTKjhio18CCjc7QHV870_erkD9fNo_Vi1qPeT3Sb-8eO8h39WtM4cZ8Ro-
TeoQRAfXg2DHC40kyFY9YlyC_zIEvnGQBwOWlw5Z7_di1b1JUD9sxuOAXPnLw5FsSuT_j_nzqk6Jv20jOu-bssIywBf,
    ssl_validate_server=1,
    timeout=60,
    outgoing_proxy=(null),
    pass_cookies=0,
    ssl_cert=(null),
    ssl_key=(null),
    ssl_key_pwd=(null),
referer: https://idp2.local/
```

OP: eingehender UserInfo Request

```
==> /var/log/apache2/access-idp2.log <==
127.0.0.3 - - [20/Apr/2023:15:59:56 +0200] "GET /idp/profile/oidc/userinfo HTTP/1.1" 200 3965 "-" "mod_auth_openidc"
```

OP: UserInfo Response

```
==> logs/idp-process.log <==
2023-04-20 15:59:57,455 - 127.0.0.3 - INFO [Shibboleth-Audit.OIDC.UserInfo:338] – 127.0.0.3|2023-04-20T13:59:56.967591Z|
    2023-04-20T13:59:57.454867Z|professorin|_71f6d421627e10f91b17be9736ccafe9||||sub,email_verified,name,
    preferred_username,given_name,family_name,email|5241e5ad778e6a9de03336337da47ddaabf354ecd3deaa0913518eb7647398cb|
    ||||UserInfoRequest|UserInfoSuccessResponse|||||mod_auth_openidc
```

RP: UserInfo erhalten

```
[Thu Apr 20 15:59:57.555901 2023] [auth_openidc:debug] [pid 6819] src/proto.c(2145): [client 127.0.0.1:44868]
oidc_user_info_response_validate: successfully decrypted JWE returned from userinfo endpoint:{
    "sub":"5241e5ad778e6a9de03336337da47ddaabf354ecd3deaa0913518eb7647398cb",
    "email_verified":false,
    "name":"Maria Pingel",
    "preferred_username":"professorin",
    "given_name":"Maria",
    "family_name":"Pingel",
    "email":"maria.pingel@nodomain.local"
}, referer: https://idp2.local/
```

RP: Zusammenführen der Token-Informationen

```
[Thu Apr 20 15:59:57.556114 2023] [auth_openidc:debug] [pid 6819] src/util.c(2240): [client 127.0.0.1:44868]
oidc_util_json_merge: result dst={
    "sub":"5241e5ad778e6a9de03336337da47ddaabf354ecd3deaa0913518eb7647398cb",
    "email_verified":false,
    "name":"Maria Pingel",
    "preferred_username":"professorin",
    "given_name":"Maria",
    "family_name":"Pingel",
    "email":"maria.pingel@nodomain.local",
    "at_hash":"mSGiXlf3yodv4X3On3gF8Q",
    "aud":"_71f6d421627e10f91b17be9736ccafe9",
    "auth_time":1681999191,
    "iss":"https://idp2.local",
    "exp":1682002796,
    "iat":1681999196,
    "nonce":"yO00nscthS_oHoxWvxiGAJtwBjK8NCZgrGTpjUQXn1k",
    "sid":"_a7ccdf74d25c45fd0bd979a70788e9e0"
}, referer: https://idp2.local/
```

RP: Zugriff auf geschützte Ressource im Namen des Resource Owners

```
127.0.0.1 - 5241e5ad778e6a9de03336337da47ddaabf354ecd3deaa0913518eb7647398cb [20/Apr/2023:15:59:57 +0200] "GET /valid-user/ HTTP/1.1" 200 2400 "https://idp2.local/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0"
```

Logdatei von OP mit optionaler Tokenverschlüsselung (Ausschnitt)

OP: Verschlüsselung am Bsp. der UserInfo Response

```
2023-05-09 14:42:58,388 - 127.0.0.2 - DEBUG
[net.shibboleth.idp.plugin.oidc.op.profile.impl.PopulateOIDCEncryptionParameters:232] - Profile Action
PopulateOIDCEncryptionParameters: Resolving EncryptionParameters for response encryption
2023-05-09 14:42:58,389 - 127.0.0.2 - DEBUG
[net.shibboleth.idp.plugin.oidc.op.profile.impl.PopulateOIDCEncryptionParameters:291] - Profile Action
PopulateOIDCEncryptionParameters: Adding OIDC client information to resolution criteria for encryption algorithms
2023-05-09 14:42:58,397 - 127.0.0.2 - DEBUG
[net.shibboleth.idp.plugin.oidc.op.security.impl.OIDCClientInformationEncryptionParametersResolver:311] - Selected key
XnQaK2f1GYePRw7FZfPo2IU6GvuewvYdy190NDxGwq8 for alg RSA1_5 and enc A256GCM
2023-05-09 14:42:58,398 - 127.0.0.2 - DEBUG
[net.shibboleth.idp.plugin.oidc.op.profile.impl.PopulateOIDCEncryptionParameters:244] - Profile Action
PopulateOIDCEncryptionParameters: Resolved EncryptionParameters for response encryption
2023-05-09 14:42:59,204 - 127.0.0.2 - DEBUG
[net.shibboleth.idp.plugin.oidc.op.oauth2.profile.impl.AbstractEncryptTokenAction:131] - Profile Action
EncryptProcessedToken: Encrypting with kid XnQaK2f1GYePRw7FZfPo2IU6GvuewvYdy190NDxGwq8 and params alg: RSA1_5 enc:
A256GCM
```

RP: Entschlüsselung am Bsp. der UserInfo Response

```
[Tue May 09 15:03:32.854029 2023] [auth_openidc:debug] [pid 8675] src/proto.c(2112): [client 127.0.0.4:37160]
oidc_user_info_response_validate: enter: userinfo_signed_response_alg=(null), userinfo_encrypted_response_alg=RSA1_5,
userinfo_encrypted_response_enc=A256GCM, referer: https://idp1.local/
[Tue May 09 15:03:32.854596 2023] [auth_openidc:debug] [pid 8675] src/proto.c(2122): [client 127.0.0.4:37160]
oidc_user_info_response_validate: JWT header={
    "kid":"XnQaK2f1GYePRw7FZfPo2IU6GvuewvYdy190NDxGwq8",
    "cty":"JWT",
    "enc":"A256GCM",
    "alg":"RSA1_5"},
referer: https://idp1.local/
```

```
[Tue May 09 15:03:32.854979 2023] [auth_openidc:debug] [pid 8675] src/util.c(2306): [client 127.0.0.4:37160]
oidc_util_create_symmetric_key: key_len=32, referer: https://idp1.local/
[Tue May 09 15:03:32.940126 2023] [auth_openidc:debug] [pid 8675] src/proto.c(2145): [client 127.0.0.4:37160]
oidc_user_info_response_validate: successfully decrypted JWE returned from userinfo endpoint: {
    "eduPersonAssurance":"https:\\/\\/refeds.org\\/assurance",
    "sub":"5241e5ad778e6a9de03336337da47ddaabf354ecd3deaa0913518eb7647398cb",
    "schacHomeOrganization":"idp.local",
    "eduPersonScopedAffiliation":"member@local staff@local employee@local"},
referer: https://idp1.local/
```