

Programmers Guide - Serviceplatformen

Udarbejdet for:

KOMBIT A/S

Halfdansgade 8

2300 København S

Indhold

1	Introduction.....	3
2	Calling Serviceplatformen Web Services	3
2.1	InvocationContext	3
2.2	AuthorityContext.....	4
2.3	Token	5
2.4	Access Token (REST)	9
2.5	CallContext	13
3	Sample Code.....	14
3.1	Java	14
3.2	C#.....	14
3.2.1	Establish trust	14

1 Introduction

This document contains a short introduction to calling web services exposed by KOMBITs Serviceplatformen¹.

For information about specific services see the online service catalog or the document "SSE/12746/IFS/0001 Services on the Service Platform".

The reader is assumed to be familiar with SSL, Serviceplatformen self-services solution, and has established a Connection Agreement (CA) and Service Agreement (SA) to use when calling services. The reader must further have acquired a suitable SSL certificate, see below.

2 Calling Serviceplatformen Web Services

All services on Serviceplatformen are SOAP 1.1 web services, which must be called using SSL and client certificate authentication. The client certificate used when calling must be a VOCES- or FOCES certificate².

In addition to the certificate, there are three security models, some of which requires configuration of specific fields in the request. And each service can use a different combination of these models:

- InvocationContext
- AuthorityContext
- Token

2.1 InvocationContext

A service call to Serviceplatformen using InvocationContext requires specific fields. The fields identify the caller, their permissions and the service which is called in Serviceplatformen. The required fields are:

1. ServiceAgreementUUID – a unique identifier of the service agreement that the caller has made with a municipality.
2. ServiceUUID – a unique identifier of the service that the caller wants to use.
3. UserUUID – a unique identifier of the municipality on behalf of which the caller accesses the service.
4. UserSystemUUID – a unique identifier of the system that calls the service.

All of the values required for calling a service can be found by logging into the self-services solution and inspecting the service agreement.

Further, the caller can as part of the InvocationContext provide the following optional fields:

5. OnBehalfOfUser – a unique identifier of the municipality on behalf of which the caller accesses the service
6. CallersServiceCallIdentifier – an identification of the service call provided by the caller.

¹ See: <http://www.serviceplatformen.dk>

² FOCES and VOCES certificates are presently issued by NETS, see: <https://www.nets-danid.dk/>

7. AccountingInfo – a message from the caller to be used for accounting of the service call.

These last three fields are logged by Serviceplatformen to an audit log when the service is called by the caller.

An example of a call with InvocationContext:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://serviceplatformen.dk/xml/wsd1/soap11/CPRBasicInformationService/1/"
xmlns:invctx="http://serviceplatformen.dk/xml/schemas/InvocationContext/1/"
xmlns:ns2="http://serviceplatformen.dk/xml/schemas/cpr/PNR/1/">
<soapenv:Header/>
<soapenv:Body>
<ns:callCPRBasicInformationRequest>
<invctx:InvocationContext>
<invctx:ServiceAgreementUUID>43fb7e80-3f80-11e2-a32b-
d4bed98c63db</invctx:ServiceAgreementUUID>
<invctx:UserSystemUUID>17b22dc2-3f80-11e2-a32b-d4bed98c63db</invctx:UserSystemUUID>
<invctx:UserUUID>fb21b665-3f7f-11e2-a32b-d4bed98c63db</invctx:UserUUID>
<invctx:ServiceUUID>d84f1ac8-76ca-11e3-abab-138252136bdf</invctx:ServiceUUID>
<invctx:AccountingInfo>Systematic Environment Check</invctx:AccountingInfo>
<invctx:OnBehalfOfUser>OPTIONAL</invctx:OnBehalfOfUser>
<invctx:CallersServiceCallIdentifier>OPTIONAL</invctx:CallersServiceCallIdentifier>
</invctx:InvocationContext>
<ns2:PNR>0000000000</ns2:PNR>
</ns:callCPRBasicInformationRequest>
</soapenv:Body>
</soapenv:Envelope>
```

2.2 AuthorityContext

The AuthorityContext security model is the simplest way for clients to call Serviceplatformen services. It is based on CVR number and assumes that a service agreement and certificate are configured. There is one required field:

1. MunicipalityCVR – a CVR number of the municipality involved in the service agreement.

An example of call with AuthorityContext:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://serviceplatformen.dk/xml/wsd1/soap11/CPRBasicInformationService/1/"
xmlns:authctx="http://serviceplatformen.dk/xml/schemas/AuthorityContext/1/"
xmlns:callctx="http://serviceplatformen.dk/xml/schemas/CallContext/1/"
xmlns:ns2="http://serviceplatformen.dk/xml/schemas/cpr/PNR/1/">
<soapenv:Header/>
<soapenv:Body>
<ns:callCPRBasicInformationRequest>
<authctx:AuthorityContext>
<authctx:MunicipalityCVR>55133018</authctx:MunicipalityCVR>
</authctx:AuthorityContext>
<callctx:CallContext>
```

```

    <callctx:AccountingInfo>Systematic Environment Check</callctx:AccountingInfo>
    <callctx:OnBehalfOfUser>OPTIONAL</invctx:OnBehalfOfUser>
    <callctx:CallersServiceCallIdentifier>TEST</callctx:CallersServiceCallIdentifier>
  </callctx:CallContext>
  <ns2:PNR>0000000000</ns2:PNR>
</ns:callCPRBasicInformationRequest>
</soapenv:Body>
</soapenv:Envelope>

```

2.3 Token

A call to Serviceplatformen which uses the Token security model must include a token issued by the Security Token Service (STS) which is part of Støttesystemerne. You can connect with the token security model when:

1. Token is valid (signatures are correctly done by the STS and the token has not expired)
2. Token is owned by the caller (subject certificate in the token and certificate used to call Serviceplatformen are the same)
3. A valid and active service agreement is configured.
4. The entity ID in the token matches the entity ID of the called service.

An example of call with configured token:

```

<soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Header><sbef:Framework
xmlns:ns1="urn:liberty:sb:profile" xmlns:sbf="urn:liberty:sb:2006-08"
xmlns:wssu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" ns1:profile="urn:liberty:sb:profile:basic" version="2.0"
wssu:Id="_88A3984A9B482050E7148939769291219"/><Action
xmlns="http://www.w3.org/2005/08/addressing" xmlns:wssu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wssu:Id="_88A3984A9B482050E7148939769291216">http://serviceplatformen.dk/xml/wsd1/soap11/SP/D
emo/1/callDemoService</Action><MessageID xmlns="http://www.w3.org/2005/08/addressing"
xmlns:wssu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" wssu:Id="_88A3984A9B482050E7148939769291215">urn:uuid:860b5199-a212-410d-bcf4-
7ab604a6cde4</MessageID><To xmlns="http://www.w3.org/2005/08/addressing"
xmlns:wssu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"
wssu:Id="_88A3984A9B482050E7148939769291217">https://extttest.serviceplatformen.dk/service/SP/
Demo/1</To><ReplyTo xmlns="http://www.w3.org/2005/08/addressing"
xmlns:wssu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"
wssu:Id="_88A3984A9B482050E7148939769291218"><Address>http://www.w3.org/2005/08/addressing/an
onymous</Address></ReplyTo><wsse:Security xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wssu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" soap:mustUnderstand="1"><wsu:Timestamp wssu:Id="TS-
88A3984A9B482050E7148939769290911"><wsu:Created>2017-03-
13T09:34:52.909Z</wsu:Created><wsu:Expires>2017-03-
13T09:39:52.909Z</wsu:Expires></wsu:Timestamp><Assertion
xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_3d749c5f-2723-46f0-80b2-f171f4f9d08b"

```

IssueInstant="2017-03-13T09:34:52.373Z" Version="2.0"><Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://saml.adgangsstyning.eksterntest-
stoettesystemerne.dk</Issuer><Signature
xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /><SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /><Reference URI="#_3d749c5f-
2723-46f0-80b2-f171f4f9d08b" /><Transforms><Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" /><Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" /><DigestValue>IQ7VDwr0HQ0HbKrWYm3qTrrvs8
q790BoTfx6PAqtQ7w=</DigestValue></Reference></SignedInfo><SignatureValue>I8jEu4E/TtAKIfrQLwK
zCofDBUuX/Mxk/L1LMESI140oES6Pr4c6kb92n8Djkuyi0aGuJ4N6pbdok8aegLgMxRVgn3g2Fj8g3skz1Fwc1D+40tG
7z00N+wrIdE9C3Qv/hvj5+YqGeQ+o0+hRsfw5Bwm6OndkIXks4IV47fsQ+t2TmP/o3AFC9frERfdmg8iYtoG819N0Q
DJNjd2W7rchmQfMOMJgKouMz9YGkd+tJzEElCreODNF7Uva/JB311XGBcvgtwrvrhjVxk1QwZP10sinWpiKj+3QxWE0h
uqa0bXeIUzj0xRWwHc08h6t6ibUo1DY9CUCqUNjMS82Y1rg==</SignatureValue><KeyInfo><X509Data><X509Ce
rtificate>MIIGHZCCBQegAwIBAgIEUxBEhTANBgkqhkiG9w0BAQsFADBMQswCQYDVQQGEwJESzESMBAGA1UECgwJVJF
JVU1QyNDA4MSQwIgwYDVQDDbU1VTVDI0MDggU3lzdGVtdGVzdCBYSVggQ0EwHhcNMTUxMDY1NDMyWhcNMTgxMD
I4MDY1MzU2WjCBjTELMAkGA1UEBhMCRESxIzAhBgNVBAoMGTPTUJJCWBBL1MgLy8gQ1ZSOjE5NDM1MDC1MvkwIAYDVQ
QFEx1DV1I6MTk0MzUwNzUtRk1EOjUwOTcwMzk5MDUGA1UEAwuS09NQk1UIFN0w7h0dGVzeXN0ZW1lc1UIChmdW5rdG
1vbnNjZXJ0aWZpa2F0KTCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIuiioynjsh/kimXd0YiYyxJANHhsp6
k9GCzc0NgR0mnD3hyofV0bCizG3irBRisY4Xn6NXBaEDz4oR5QUa7g/f3tI4Z5Z123egcz0h3pur4k0jnpAjuKjLnLd
g2WJadZsydUC69uwyhZnjQS9RLZ90wPWA0INwQzjN/w4s4AA6Vn4JpLdoGU//hiAzMzZDn+y1YZUmiaDtSuNpE4Roh8Y
742rpdAoW6NZIRp5Jg1XRSJNMnY0b0Sy3wu0YCh7eyq4AB/5p6Qw16xMpr3TZbQK09rXw5ZpuCLhncWtaZehI/ibZBBY
kwEu+1w/BuPu7xBT8S40+2CQuFpBd8Pr6tbJ8CAwEAa0CAsovgLGMGA4GA1UdDwEB/wQEAWIDuDCBlwYIKwYBBQUHAQ
EEgYowgYcwPAYIKwYBBQUHMAAGGMGh0dHA6Ly9vY3NwLnN5c3R1bXRlc3QxOS50cnVzdDI0MDguY29tL3Jlc3Bvbmlc
BHBggrBgEFBQcwAoY7aHR0cDovL2YuYW1hLnN5c3R1bXRlc3QxOS50cnVzdDI0MDguY29tL3N5c3R1bXRlc3QxOS51jYS
5jZXIwggEgBgNVHSAEAggEXMIIBEzCCAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cuZm
Jlc3QyNDA4LmNvbS5yZXBvc210b3J5MIHJBGgrBgEFBQcCAjCBvDAMFgVEYw5JRDAADAgEBG0GrRGFuSUQgdGVzdCBjZX
J0aWZpa2F0ZXIgzNjJhIGRlbn51IENBIHVkc3R1ZGVzIHVzZGVyIE9JRCAxLjMuNi4xLjQUMS4zMTMxMy4yLjQUMi40Lj
IuIERhbklEIERlc3QyY2VydG1maWnhdGVzIGZyb20gdGhpcyBDQSBhcmUgaXNzdWVkIHVzZGVyIE9JRCAxLjMuNi4xLj
QUMS4zMTMxMy4yLjQUMi40LjIuMIGqBgNVHR8EgaIwZ8wPKA6oDiGNmh0dHA6Ly9jcmwuc3lzdGVtdGVzdDE5LnRydX
N0MjQwOC5j20vc3lzdGVtdGVzdDE5LmNybDBfoF2gW6RZMFcxCAZJBGNVBAYTAkRMLRIwEAYDVQQKDA1U1VTVDI0MD
gxJDAiBgNVBAMMG1RSVVNUMjQwOCBTEhN0ZW10ZXN0IFhJWCBDQTEOMAwGA1UEAwuS09NQk1U1MNDQwHwYDVR0jBBgwFoAUZA
JVDOSBdk8gVNURFFeckVI4f6AwHQYDVR00BBYEFcQbh/pb3R7yKQytvLeA5XE0FVxjMAkGA1UdEwQCAAwDQYJKoZIhvc
NAQELBQADggEBACoRkbV6V45GX5uXmtZzFTSc/ycRD3CoPSFTqCQR3cMwBE/ERJ8b+0b8K51hsEyK7NSGPTxz158Nb
tPd+g2HqRmX0hOvchbzVRonudDb2vuaa4k5CxxhUhzXockPNo6phwhf11NMR0cSFKMyq+s/Sf41QMA3GKe9KofGhDi2DC
AAAtVGz9nBHIAEQW+Tvj8IYYQ4wKVvfBGp02lWNCEmepRGZkdObNLHntis39uYezrnMpXuw9nzn07km5408eG928HfcNN
Hg9omuGhG/y5axGYMM5La1C9dNRAC0JMTiULBfHMVA1Mzm8WmGsk4mof5/VcbRmE2AHJ0wNricpzzAxpG=</X509Cert
ificate></X509Data></KeyInfo></Signature><Subject><NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">SERIALNUMBER=CVR:19435075-FID:37671533 + CN=kombit-sp-t-demo-serv
(funktionscertifikat), 0=KOMBIT A/S // CVR:19435075, C=DK</NameID><SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key"><SubjectConfirmationData
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" NotBefore="2017-03-13T09:34:52.373Z"
NotOnOrAfter="2017-03-13T10:34:52.373Z" Recipient="http://demo.prod-
serviceplatformen.dk/service/DemoService/1" a:type="KeyInfoConfirmationDataType"><KeyInfo
xmlns="http://www.w3.org/2000/09/xmldsig#"><X509Data><X509Certificate>MIIGHDCBQSwAwIBAgIEVp
63zDANBgkqhkiG9w0BAQsFADBMQswCQYDVQQGEwJESzESMBAGA1UECgwJVJFJVU1QyNDA4MSQwIgwYDVQDDbU1VTVD
I0MDggU3lzdGVtdGVzdCBYSVggQ0EwHhcNMTUxMDY1NDMyWhcNMTgxMDY1NDMyWhcNMTgxMDY1NDMyWhcNMTgxMDY1NDMy
sxIzAhBgNVBAoMGTPTUJJCWBBL1MgLy8gQ1ZSOjE5NDM1MDC1MvYywhcNMTgxMDY1NDMyWhcNMTgxMDY1NDMyWhcNMTgxMDY1NDMy
cxNTMzMDIGA1UEAwuS09NQk1U1MNDQwHwYDVR0jBBgwFoAUZAJVDOSBdk8gVNURFFeckVI4f6AwHQYDVR00BBYEFcQbh/pb3R7yKQytvLeA5XE0FVxjMAkGA1UdEwQCAAwDQYJKoZIhvcNAQELBQADggEBACoRkbV6V45GX5uXmtZzFTSc/ycRD3CoPSFTqCQR3cMwBE/ERJ8b+0b8K51hsEyK7NSGPTxz158NbtPd+g2HqRmX0hOvchbzVRonudDb2vuaa4k5CxxhUhzXockPNo6phwhf11NMR0cSFKMyq+s/Sf41QMA3GKe9KofGhDi2DCAAAtVGz9nBHIAEQW+Tvj8IYYQ4wKVvfBGp02lWNCEmepRGZkdObNLHntis39uYezrnMpXuw9nzn07km5408eG928HfcNNHg9omuGhG/y5axGYMM5La1C9dNRAC0JMTiULBfHMVA1Mzm8WmGsk4mof5/VcbRmE2AHJ0wNricpzzAxpG=</X509Certificate></X509Data></KeyInfo></Signature><Subject><NameID


```
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="soap"/></ds:CanonicalizationMethod><ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/><ds:Reference URI="#TS-
88A3984A9B482050E7148939769290911"><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="wsse
soap"/></ds:Transform></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>3h+TyCqbOT0XbPvVHbMIP1Y
BZw7jyNXRz0h5dbbLeNw=</ds:DigestValue></ds:Reference><ds:Reference URI="#STR-
88A3984A9B482050E7148939769291113"><ds:Transforms><ds:Transform
Algorithm="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#STR-Transform"><wsse:TransformationParameters><ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/></wsse:TransformationParameters></ds:Transform></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>FLiMyS00Wv8KIde9J/e0x1E
Hma66x3TgOnguUOATw38=</ds:DigestValue></ds:Reference><ds:Reference
URI="#_88A3984A9B482050E7148939769291214"><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList=""></ds:Transform></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>C71y+Q1CkcBvUIInHW3N67Ar
5JxEyrLvMZJHfcb6rxIY=</ds:DigestValue></ds:Reference><ds:Reference
URI="#_88A3984A9B482050E7148939769291215"><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="soap"/></ds:Transform></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>Tv438EXugA4j60Uj2t0dwwP
i1lvLnkWSaazcCeDJNX8=</ds:DigestValue></ds:Reference><ds:Reference
URI="#_88A3984A9B482050E7148939769291216"><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="soap"/></ds:Transform></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>a/01kt4PtU5wevqmqjXuqMkT
IIWfX7G9v9cAKYogog1nc=</ds:DigestValue></ds:Reference><ds:Reference
URI="#_88A3984A9B482050E7148939769291217"><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="soap"/></ds:Transform></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>qCXteleHXFWCU6w9sCTJU5I
ZLxfeeRppMIrI0n0sf3w=</ds:DigestValue></ds:Reference><ds:Reference
URI="#_88A3984A9B482050E7148939769291218"><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="soap"/></ds:Transform></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>OqWOAd1+tUQCgUKTt1ByBDB
XwdotM8z5YfxXbE5GXG4=</ds:DigestValue></ds:Reference><ds:Reference
URI="#_88A3984A9B482050E7148939769291219"><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="soap"/></ds:Transform></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>aUo1Fr8rPDY4QwuqF3IwG62
```

```
cNuSXWskzLSjrCjKspkw=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>IHcD
zMXCXWtJQrvuSOPgl3eGHv+/DzmfdfmSkXxrQ+hLbjsWd4Uoidvr6WWqGwrfipHyMwiBGWAwLUAcrL8c+Nz3Q6VeC0
o+/RwRDU8pzQgaODk61847By8gFBkMbcVtoGSZQxpoYrJcJnltw2IYo1xA/bdLOEGSSwr/2h42uCFgjeRaoFuQxcU7o
M2XCoV5i0xDovJfjtnk1Zn4+YafmQIusrHyIKk1e25GRFtBh1RbfWUkpqKD2zkv7/Xg8LiV9kyH49LoR2f7Ki6/aVY1L
glfzZvK1JxGub10bpCWJG3kCT5RERkIHyeu+TQHfwys7Msn1rFQ0f3wJDTqqyQ==</ds:SignatureValue><ds:KeyI
nfo Id="KI-88A3984A9B482050E7148939769291320"><SecurityTokenReference
xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:b="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
b:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0"><KeyIdentifier Value="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.1#SAMLID">_3d749c5f-2723-46f0-80b2-
f171f4f9d08b</KeyIdentifier></SecurityTokenReference></ds:KeyInfo></ds:Signature></wsse:Secu
rity></soap:Header><soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="_88A3984A9B482050E7148939769291214"><ns4:CallDemoServiceRequest
xmlns="http://serviceplatformen.dk/xml/schemas/CallContext/1/"
xmlns:ns2="http://serviceplatformen.dk/xml/schemas/AuthorityContext/1/"
xmlns:ns3="http://serviceplatformen.dk/xml/schemas/InvocationContext/1/"
xmlns:ns4="http://serviceplatformen.dk/xml/wsd1/soap11/SP/Demo/1/"
xmlns:ns5="http://serviceplatformen.dk/xml/schemas/ServiceplatformFault/1/"><CallContext><On
BehalfOfUser>behalfOfUser</OnBehalfOfUser><CallersServiceCallIdentifier>callersIdentifier</C
allersServiceCallIdentifier><AccountingInfo>5e708ef0-1e47-4340-816c-
a1e91447d831</AccountingInfo></CallContext><ns4:messageString>test</ns4:messageString></ns4:
CallDemoServiceRequest></soap:Body></soap:Envelope>
```

2.4 Access Token (REST)

RESTful web services offered by Serviceplatformen require a token issued by the Security Token Service (STS). For SOAP services the token is included in the service request (cf. section 2.2), while RESTful services are modelled over Digitaliseringsstyrelsen's OIO IDWS REST Profile V1.0 (<https://www.digitaliser.dk/resource/3457606>), which requires that the client performs the following sequence:

1. Calls STS to obtain a SAML token
2. Calls Serviceplatformen's Access Token Service to exchange the (large, ca. 8 KB) SAML Token for a (small – UUID formatted) Access Token
3. Calls the intended RESTful service offered by Serviceplatformen including the Access Token as an HTTP header

As a result of step 2., Serviceplatformen stores the SAML token associated with the Access Token for the validity period of the SAML token.

As a result of step 3., Serviceplatformen matches the Access Token from the request with the SAML token received in step 2. and performs access control based on the contents of the token following the same policies as for SOAP services (cf. section 2.2).

Serviceplatformen allows repeated calls to RESTful services (Step 3.) covered by the scope of the SAML token with the same Access Token during the validity period of the SAML token.

The response from the Access Token service will be a UUID-formatted identifier returned in a JSON-formatted payload. Fx.

```
HTTP/1.1 200 OK
Date: Fri, 09 Jul 2021 11:12:27 GMT
Server: Apache-Coyote/1.1
Content-Type: application/json
Connection: Keep-Alive
Transfer-Encoding: chunked
```

```
{"access_token":"5fc9df8d-f81e-497b-bb69-5f8aca4017cc","token_type":"Holder-Of-Key","expires_in":3600}
```

The RESTful service in step 3. will require the UUID-formatted Access Token included as the value of the Authorization header in the request as Holder-of-key.

In the Serviceplatformen ExtTest environment an example of such a service, AccessTokenDemoService, is offered for demo purposes. It is offered under the same service agreement as the SOAP DemoService referred in the previous sections. The examples below refer to this service.

```
GET /service/AccessTokenDemo_1/callDemoService/TestingSuccessfulResponse HTTP/1.1
Host: <env>.serviceplatformen.dk
x-TransaktionsId: 123456
x-TransaktionsTid: 2021-07-09T10:15:30+01:00[Europe/Paris]
Authorization: Holder-of-key 5fc9df8d-f81e-497b-bb69-5f8aca4017cc
```

The headers x-TransaktionsId and x-TransaktionsTid are mandatory and must be generated by the client to comply with KOMBIT's transaction trace standards. They are echoed as response headers by the RESTful service. Fx.

```
HTTP/1.1 200 OK
Content-Length: 13
content-type: application/json
Date: Fri, 09 Jul 2021 12:19:01 GMT
Keep-Alive: timeout=5, max=100
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
x-TransaktionsId:123456
x-TransaktionsTid: 2021-07-09T10:15:30+01:00[Europe/Paris]
```

```
{"data":"OK"}
```

2.5 CallContext

There is also an optional tag CallContext which consists the fields *OnBehalfOfUser*, *CallersServiceCallIdentifier* and *AccountingInfo* (Description to these fields can be found under InvocationContext). The CallContext can be used along with the Authority and Token security models, but it's not mandatory. And those fields are also present as an optional part of InvocationContext.

3 Sample Code

As part of this programmer's guide, small samples illustrating how to call a service on Serviceplatformen are available in both Java and C#.

The samples can run out of the box, as a connection agreement, service agreement and OCES certificate have already been setup in the environment (exttest). The demo clients can only run against the exttest environment. To make a client for another service run against the production environment OCES certificates intended for production environments should be used and the URL defining the endpoint should be changed.

Demo clients were created to provide an example how to implement clients which can connect to Serviceplatformen. The Demo Service on Serviceplatformen side is just an echo service and responds with the same message which was sent in the request.

3.1 Java

The sample client can be found here: <https://github.com/Serviceplatformen>

Instructions for running the clients can be found in the readme.md show on the repository's main page. The java client repository contains three clients

- one for the context based security models (AuthorityContext and InvocationContext)
- one for the token (SOAP) based security model.
- one for the Access Token (REST) based security model.

For more details, please see the repository.

3.2 C#

The sample client can be found here: <https://github.com/Serviceplatformen>

Instructions for running the clients can be found in the readme.md show on the repository's main page. The C# client repository contains two clients, one for the context based security models (AuthorityContext and InvocationContext) and one for the token based security model. For more details, please see the repository.

3.2.1 Establish trust

To call services, it is necessary to establish trust to Serviceplatformen. This is done in 2 steps.

- 1) Download and save the server certificate from the environment you wish to run on (<https://exttestwww.serviceplatformen.dk> or <https://www.serviceplatformen.dk>). This may be done via a web browser, for instance Mozilla Firefox.
- 2) Add the downloaded certificate into your trust store (can be done using mmc.exe, see [http://msdn.microsoft.com/en-us/library/bb950259\(v=bts.10\).aspx](http://msdn.microsoft.com/en-us/library/bb950259(v=bts.10).aspx) for usage of this tool)