Creating a SAML token, step-by-step

1. Create a certificate using makecert

C:\Dialog>makecert -r -pe -n "CN=SamlTokenSigningCertificate" -b 11/16/2014 -e 01/01/2020 -sky exchange SamlTokenSigningCertificate.cer -sv SamlTokenSigningCertificate.pvk

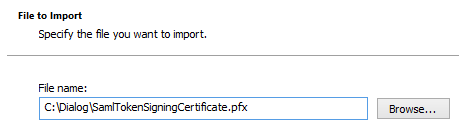
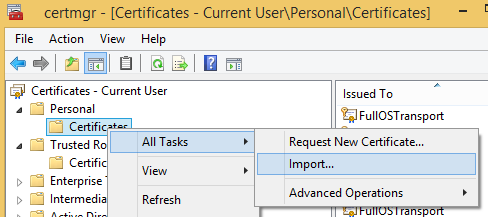
(2 x password set: 123)

Succeeded

C:\Dialog>pvk2pfx.exe -pvk SamlTokenSigningCertificate.pvk -spc SamlTokenSigningCertificate.cer -pfx SamlTokenSigningCertificate.pfx

(Password asked: 123)

1. Import this certificate (the pfx one, because we need to include the private key also)



1. Create a console application with following code:

class Program

{

static void Main(string[] args)

{

var claims = new WindowsClaimSet(WindowsIdentity.GetCurrent());

using (claims)

{

foreach (var claim in claims)

{

Console.WriteLine(string.Format("Claim Type: {0}", claim.ClaimType));

Console.WriteLine(string.Format("Resource: {0}", claim.Resource));

Console.WriteLine(string.Format("Right: {0}", claim.Right));

}

var accessControlClaims = claims.FindClaims(ClaimTypes.Sid,   
 Rights.PossessProperty);

var assertion =   
 CreateSamlAssertionFromWindowsIdentityClaims(accessControlClaims);

var token = new SamlSecurityToken(assertion);

SerializeSamlTokenToFile(token);

Console.ReadKey();

}

}

private static SamlAssertion   
 CreateSamlAssertionFromWindowsIdentityClaims(IEnumerable<Claim> claims)

{

var subject = new SamlSubject()

{

Name = "Windows Group Claim"

};

var statement = new SamlAttributeStatement()

{

SamlSubject = subject

};

var assertion = new SamlAssertion()

{

AssertionId = string.Format("\_{0}", Guid.NewGuid().ToString()),

Issuer = "System"

};

foreach (var claim in claims)

{

var samlClaim = new Claim(claim.ClaimType, GetResourceFromSid(  
 claim.Resource as SecurityIdentifier), claim.Right);

var attribute = new SamlAttribute(samlClaim);

statement.Attributes.Add(attribute);

}

assertion.Statements.Add(statement);

SignSamlAssertion(assertion);

return assertion;

}

private static string GetResourceFromSid(SecurityIdentifier sid)

{

try

{

return sid.Translate(typeof(NTAccount)).ToString();

}

catch (Exception)

{

return sid.Value;

}

}

private static void SignSamlAssertion(SamlAssertion assertion)

{

var certificate2 = GetCertificateFromStore(StoreLocation.CurrentUser,   
 DateTime.Now, "CN=SamlTokenSigningCertificate");

if (certificate2 != null)

{

var securityKey = new X509AsymmetricSecurityKey(certificate2);

assertion.SigningCredentials = new SigningCredentials(

securityKey,

SecurityAlgorithms.RsaSha1Signature,

SecurityAlgorithms.Sha1Digest,

new SecurityKeyIdentifier(  
 new X509ThumbprintKeyIdentifierClause(certificate2)));

}

}

private static X509Certificate2 GetCertificateFromStore(StoreLocation location,   
 DateTime timeValid, string subjectDistinguishedName)

{

var store = new X509Store(location);

try

{

store.Open(OpenFlags.ReadOnly);

var validCertificates = store.Certificates.Find(X509FindType.FindByTimeValid,   
 timeValid, false);

var signingCertificate =   
 validCertificates.Find(X509FindType.FindBySubjectDistinguishedName,   
 subjectDistinguishedName, false);

if (signingCertificate.Count == 0)

return null;

return signingCertificate[0];

}

finally

{

store.Close();

}

}

private static void SerializeSamlTokenToFile(SamlSecurityToken token)

{

using (var writer = XmlWriter.Create(@"C: \Dialog\saml.xml"))

{

try

{

var keyInfoSerializer = new WSSecurityTokenSerializer();

keyInfoSerializer.WriteToken(writer, token);

Console.WriteLine("Saml Token Successfully Created");

}

catch (Exception ex)

{

string s1 = ex.Message;

string s2 = ex.InnerException.Message;

string s3 = ex.InnerException.InnerException.Message;

string s4 = ex.InnerException.InnerException.InnerException.Message;

Console.WriteLine("Failed to save Saml Token to Disk");

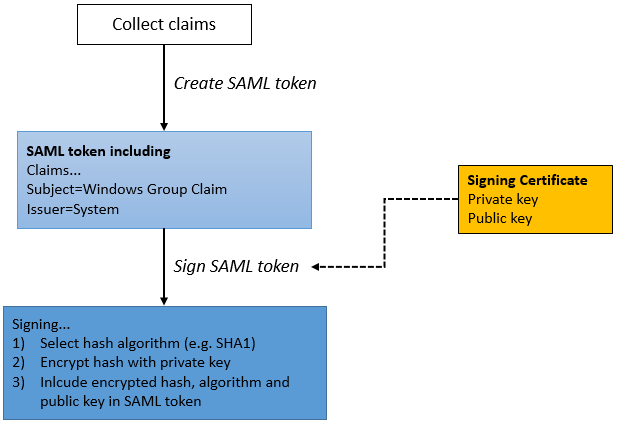
}

}

}

}

1. Diagram



1. SAML content:

<?xml version="1.0" encoding="utf-8"?>

<saml:Assertion MajorVersion="1" MinorVersion="1" AssertionID="\_40882b7d-e965-4dfa-ac22-6562d529ec71" Issuer="System" IssueInstant="2014-11-17T14:33:15.765Z" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">

<saml:AttributeStatement>

<saml:Subject>

<saml:NameIdentifier>Windows Group Claim</saml:NameIdentifier>

</saml:Subject>

<saml:Attribute AttributeName="sid" AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">

<saml:AttributeValue>ALEJANDROAM3845\alejandroamrein</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute AttributeName="sid" AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">

<saml:AttributeValue>ALEJANDROAM3845\None</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute AttributeName="sid" AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">

<saml:AttributeValue>Everyone</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute AttributeName="sid" AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">

<saml:AttributeValue>BUILTIN\Hyper-V Administrators</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute AttributeName="sid" AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">

<saml:AttributeValue>BUILTIN\Performance Log Users</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute AttributeName="sid" AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">

<saml:AttributeValue>BUILTIN\Users</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute AttributeName="sid" AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">

<saml:AttributeValue>NT AUTHORITY\INTERACTIVE</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute AttributeName="sid" AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">

<saml:AttributeValue>CONSOLE LOGON</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute AttributeName="sid" AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">

<saml:AttributeValue>NT AUTHORITY\Authenticated Users</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute AttributeName="sid" AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">

<saml:AttributeValue>NT AUTHORITY\This Organization</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute AttributeName="sid" AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">

<saml:AttributeValue>NT AUTHORITY\Local account</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute AttributeName="sid" AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">

<saml:AttributeValue>LOCAL</saml:AttributeValue>

</saml:Attribute>

<saml:Attribute AttributeName="sid" AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">

<saml:AttributeValue>NT AUTHORITY\NTLM Authentication</saml:AttributeValue>

</saml:Attribute>

</saml:AttributeStatement>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">

<SignedInfo>

<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></CanonicalizationMethod>

<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></SignatureMethod>

<Reference URI="#\_40882b7d-e965-4dfa-ac22-6562d529ec71">

<Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></Transform>

<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transform>

</Transforms>

<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>

<DigestValue>/dNiTR7UuC/URfJOIlcshVO3/2k=</DigestValue>

</Reference>

</SignedInfo>

<SignatureValue>DfR2L7Nqou54UbAQaPCiQea1T2sLk5lXju8Nv5HPQ4YxWQh0UNMb2UCtJEGd2xZA5D4pWgqCLmn0qD3vhXR0HzpCcshD38+c3aZpCt9gJjh+itHzEpukXHXlP3t0YWU8Kchqj79FneGXPyxR6dRCPy7BONzAvu6vbh+fZ2UylEborQ75UUKD3MuYmTI+/byxdLsX2RcN8oc2ntoLorlhSkIDDlw9pBgO/XW2DyLSdG+1i9i4x4iSWyL/6JVK2eA0bBZMXc1ERUjUL87WyHzYxmQoE4x2CSeYOs6p0adFAM0Swba8UsiGgK/oevjLmAyciV5wcks3cuYZauzxsN1fvA==</SignatureValue>

<KeyInfo>

<o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">

<o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#ThumbprintSHA1">2RFUTt1vm4aTGQFv6yFRVJQfyjQ=</o:KeyIdentifier>

</o:SecurityTokenReference>

</KeyInfo>

</Signature>

</saml:Assertion>

1. nn