

Re: Encrypt a UsernameToken Authenticated WSE Response

>> so as long as you are passing a password digest,
>> then a hacker cannot generate that key without knowing the password.
>> that password should already be a shared secret between the client and
>> server,
>> and is just used to generate the session key to encrypt.
>> the session key will be different each time because of the nonce and
>> date.
>>
>> Thanks,
>> casey
>> <http://www.brains-N-brawn.com>
>>
>>
>> "AndiRudi" <AndiRudi@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
>> news:5CDFC579-18F5-4D5C-808E-8C6D25013CB4@xxxxxxxxxxxxxxxxxxxx
>> > One additional question:
>> >
>> > how is the data secured now? I think that the key is a kombination from
>> > username and passwort und the data is symmetric encrypted, but then a
>> > hacker
>> > can read that values and decrypt it?
>> >
>> > "AndiRudi" wrote:
>> >
>> >> OK i got it :) Will make an artichel about that soon
>> >>
>> >> "AndiRudi" wrote:
>> >>
>> >> > Thanks,
>> >> >
>> >> > meanwhile i tried the Examples in the WSE2 Documentation named
>> >> > "Encrypt
>> >> > (or
>> >> > Decrypt) a SOAP Message by Using a Username and Password". I send my
>> >> > Password
>> >> > hashed and also habe a working AuthenticateUser method overwritten
>> >> > und
>> >> > registered in web.config. But when I start my Client Application and
>> >> > call my
>> >> > HelloWorld() method i get an Exception... Mutable Security Token has
>> >> > to
>> >> > be
>> >> > added into the tokens collection. I even have no Trace thats a big
>> >> > problem.
>> >> > I've switched on the Trace in both projects and have set all
>> >> > Directory
>> >> > write
>> >> > accesses but there are still no trace files.
>> >> >
>> >> > Codes: (<http://localhost/WSETest/service1.asmx> and my client app is
>> >> > in

Re: Encrypt a UsernameToken Authenticated WSE Response

```
>>>> wroot/wseclient)
>>>>
>>>> client:
>>>> WSEClient.localhost.Service1Wse proxy = new localhost.Service1Wse();
>>>> UsernameToken userToken = new UsernameToken("Andreas",
>>>> "test",PasswordOption.SendHashed);
>>>> EncryptedData encrypt = new EncryptedData(userToken);
>>>> proxy.RequestSoapContext.Security.Elements.Add(encrypt);
>>>> proxy.RequestSoapContext.Security.Timestamp.TtlInSeconds = 300;
>>>> MessageBox.Show(proxy.HelloWorld());
>>>>
>>>> clientpolicy:
>>>> <?xml version="1.0" encoding="utf-8"?>
>>>> <policyDocument
>>>> xmlns="http://schemas.microsoft.com/wse/2003/06/Policy>
>>>> <mappings
>>>> xmlns:wse="http://schemas.microsoft.com/wse/2003/06/Policy>
>>>> <endpoint uri="http://localhost/WSETests/Service1.asmx>
>>>> <defaultOperation>
>>>> <request
>>>> > policy="#policy-c0a22319-6b89-49ff-9b82-bdbac5f04618"
>>>> />
>>>> <response policy="" />
>>>> <fault policy="" />
>>>> </defaultOperation>
>>>> </endpoint>
>>>> </mappings>
>>>> <policies
>>>> > xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
>>>> <wsp:Policy wsu:Id="policy-c0a22319-6b89-49ff-9b82-bdbac5f04618"
>>>> xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy
>>>> xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing>
>>>> <wssp:Confidentiality wsp:Usage="wsp:Required"
>>>> xmlns:wssp="http://schemas.xmlsoap.org/ws/2002/12/secext>
>>>> <wssp:KeyInfo>
>>>> <SecurityToken
>>>> xmlns="http://schemas.xmlsoap.org/ws/2002/12/secext>
>>>>
>>>>
>>>> > <wssp:TokenType>http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-user
>>>> > name-token-profile-1.0#UsernameToken</wssp:TokenType>
>>>> <wssp:Claims>
>>>> <wssp:UsePassword Type="wssp:PasswordDigest"
>>>> wsp:Usage="wsp:Required" />
>>>> </wssp:Claims>
>>>> </SecurityToken>
>>>> </wssp:KeyInfo>
>>>> <wssp:MessageParts
>>>> > Dialect="http://schemas.xmlsoap.org/2002/12/wsse#part>
```

Re: Encrypt a UsernameToken Authenticated WSE Response

```
>>>> wsp:Body()
>>>> </wssp:MessageParts>
>>>> </wssp:Confidentiality>
>>>> </wsp:Policy>
>>>> </policies>
>>>> </policyDocument>
>>>>
>>>> service:
>>>> [WebMethod]
>>>> public string HelloWorld()
>>>> {
>>>> //Get the current soap context
>>>> SoapContext ctxt = RequestSoapContext.Current;
>>>> if (ctxt == null) { return "Please format the request as a SOAP
>>>> request and try again.";
>>>> }
>>>>
>>>> //Iterate through all Security tokens
>>>> foreach(SecurityToken tok in ctxt.Security.Tokens){
>>>> if (tok is UsernameToken) {
>>>> UsernameToken user = (UsernameToken)tok;
>>>> return "Hello Authenticated user " + user.Username;
>>>> }
>>>> }
>>>> return "Hello Liar";
>>>> }
>>>>
>>>> ServicePolicy:
>>>> <?xml version="1.0" encoding="utf-8"?>
>>>> <policyDocument
>>>> xmlns="http://schemas.microsoft.com/wse/2003/06/Policy>
>>>> <mappings
>>>> xmlns:wse="http://schemas.microsoft.com/wse/2003/06/Policy>
>>>> <endpoint uri="http://localhost/WSETests/Service1.asmx>
>>>> <defaultOperation>
>>>> <request
>>>> policy="#policy-c0a22319-6b89-49ff-9b82-bdbac5f04618"
>>>> />
>>>> <response policy="" />
>>>> <fault policy="" />
>>>> </defaultOperation>
>>>> </endpoint>
>>>> </mappings>
>>>> <policies
>>>>
>>>> xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurit
>>>> y-utility-1.0.xsd">
>>>> <wsp:Policy wsu:Id="policy-c0a22319-6b89-49ff-9b82-bdbac5f04618"
>>>> xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy
>>>> xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing>
>>>> <wssp:Confidentiality wsp:Usage="wsp:Required"
```

Re: Encrypt a UsernameToken Authenticated WSE Response

```
>>>> xmlns:wssp="http://schemas.xmlsoap.org/ws/2002/12/secext">
>>>> <wssp:KeyInfo>
>>>> <SecurityToken
>>>> xmlns="http://schemas.xmlsoap.org/ws/2002/12/secext">
>>>>
>>>>
>>>> <wssp:TokenType>http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-user
>>>> name-token-profile-1.0#UsernameToken</wssp:TokenType>
>>>> <wssp:Claims>
>>>> <wssp:UsePassword Type="wssp:PasswordDigest"
>>>> wsp:Usage="wsp:Required" />
>>>> </wssp:Claims>
>>>> </SecurityToken>
>>>> </wssp:KeyInfo>
>>>> <wssp:MessageParts
>>>> Dialect="http://schemas.xmlsoap.org/2002/12/wsse#part">
>>>> wsp:Body()
>>>> </wssp:MessageParts>
>>>> </wssp:Confidentiality>
>>>> </wsp:Policy>
>>>> </policies>
>>>> </policyDocument>
>>>>
>>>> Maybe you or anyone see's the failure.
>>>> Thanks, trying that for 3 days now...
>>>>
>>>>
>>>>
>>>> "casey chesnut" wrote:
>>>>
>>>>> you can encrypt with a UsernameToken too.
>>>>> both the client and the server know the password,
>>>>> so that is used to generate a key to encrypt with.
>>>>>
>>>>> on the client Request you add something like this line:
>>>>> serviceProxy.RequestSoapContext.Security.Elements.Add(new
>>>>> EncryptedData(token));
>>>>>
>>>>> the server Response adds something like this :
>>>>> ResponseSoapContext.Current.Security.Tokens.Add(usernameToken);
>>>>> ResponseSoapContext.Current.Security.Elements.Add(new
>>>>> MessageSignature(usernameToken));
>>>>> ResponseSoapContext.Current.Security.Elements.Add(new
>>>>> EncryptedData(usernameToken));
>>>>>
>>>>> Thanks,
>>>>> casey
>>>>> http://www.brains-N-brawn.com
>>>>>
>>>>>
```

Re: Encrypt a UsernameToken Authenticated WSE Response

>>>>> "AndiRudi" <AndiRudi@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
>>>>> news:B7D49B82-C019-4262-BC3C-D8E3B97C8EB2@xxxxxxxxxxxxxxxxxxxx
>>>>> Is there any other possibility than x509 to encrypt a Response.
>>>>> Something
>>>>> symmetric would be nice.
>>>>>
>>>>>
>>>>>
>>>>>
>>
>>
>

-
- **Follow-Ups:**
 - ◆ **Re: Encrypt a UsernameToken Authenticated WSE Response**
 - ◇ From: William Stacey [MVP]

 - **References:**
 - ◆ **Encrypt a UsernameToken Authenticated WSE Response**
 - ◇ From: AndiRudi
 - ◆ **Re: Encrypt a UsernameToken Authenticated WSE Response**
 - ◇ From: casey chesnut
 - ◆ **Re: Encrypt a UsernameToken Authenticated WSE Response**
 - ◇ From: AndiRudi
 - ◆ **Re: Encrypt a UsernameToken Authenticated WSE Response**
 - ◇ From: AndiRudi
 - ◆ **Re: Encrypt a UsernameToken Authenticated WSE Response**
 - ◇ From: AndiRudi
 - ◆ **Re: Encrypt a UsernameToken Authenticated WSE Response**
 - ◇ From: casey chesnut
 - ◆ **Re: Encrypt a UsernameToken Authenticated WSE Response**
 - ◇ From: William Stacey [MVP]

 - Prev by Date: **Setting ReplyTo ReferenceProperties throws "The input was not a ..**
 - Next by Date: **Re: Encrypt a UsernameToken Authenticated WSE Response**
 - Previous by thread: **Re: Encrypt a UsernameToken Authenticated WSE Response**
 - Next by thread: **Re: Encrypt a UsernameToken Authenticated WSE Response**
 - **Index(es):**
 - ◆ **Date**
 - ◆ **Thread**