knowledge14®

April 27–May 1, 2014 • Moscone Center • San Francisco, CA

Integration 201: Unleash the Power of SAML 2.0

Jason Petty
Expert Services
ServiceNow

Jonatan Jardi
Senior Technical Consultant
ServiceNow

servicenow®

© 2014 ServiceNow All Rights Reserved

Jason Petty

- Expert Services for 2 years
  - Implemented SAML 60+ times
- What I do for fun
  - Model Airplanes (Building and Flying)
  - Geocaching
  - Guitar
  - Scouting
  - Golfing



© 2014 ServiceNow All Rights Reserved

Jonatan Jardi

- Technical Consultant for almost 2 years
  - Enjoy anything to do with integrations
- What I do for fun
  - Playing and watching football (soccer)
  - Going to the movies
  - Spending time with my family



© 2014 ServiceNow All Rights Reserved

Lab Agenda

- Service Provider Initiated Logon
  - Hands On Lab 1: Setup Temporary Email and SSO Circle Account
- Identity Provider (IDP) Initiated Logon
  - Hands On Lab 2: Setup Your Own SAML 2.0 Authentication
- Tools for Debugging and Troubleshooting SAML Authentication
  - Hands On Lab 3: Trace Your Own SAML 2.0 Authentication
- Demos
  - ADFS
  - Open AM
- Q & A

© 2014 ServiceNow All Rights Reserved

Lab Objectives

1. Learn how SAML 2.0 works
2. Learn how to setup and configure SAML 2.0 in a ServiceNow instance
3. Learn what tools you can use to troubleshoot

© 2014 ServiceNow All Rights Reserved

Instance Names Changed:

https://sso-001.lab.service-now.com

Password: Knowledge14

© 2014 ServiceNow All Rights Reserved

Scenario



IdP



Users

You have been asked to make ServiceNow work with the Single Sign On (SSO) solution that other applications in the company already use so users don't have to login again.

The corporate identity provider already has login credentials stored and your company wants to use the same ones to access ServiceNow



© 2014 ServiceNow All Rights Reserved

How SAML 2.0 Works

© 2014 ServiceNow All Rights Reserved

SAML 2.0 Browser POST process flow

- Service Provider (SP) Initiated Logon
  - The user goes directly to the ServiceNow instance
  - ServiceNow requests that an authentication takes place
  - ServiceNow authenticates based on a response from the corporate identity provider (IdP)
- Identity Provider (IDP) Initiated Logon
  - The user goes first to a corporate portal or identity store
  - The corporate identity store asks ServiceNow if it can launch and authenticate as a specific person

© 2014 ServiceNow All Rights Reserved

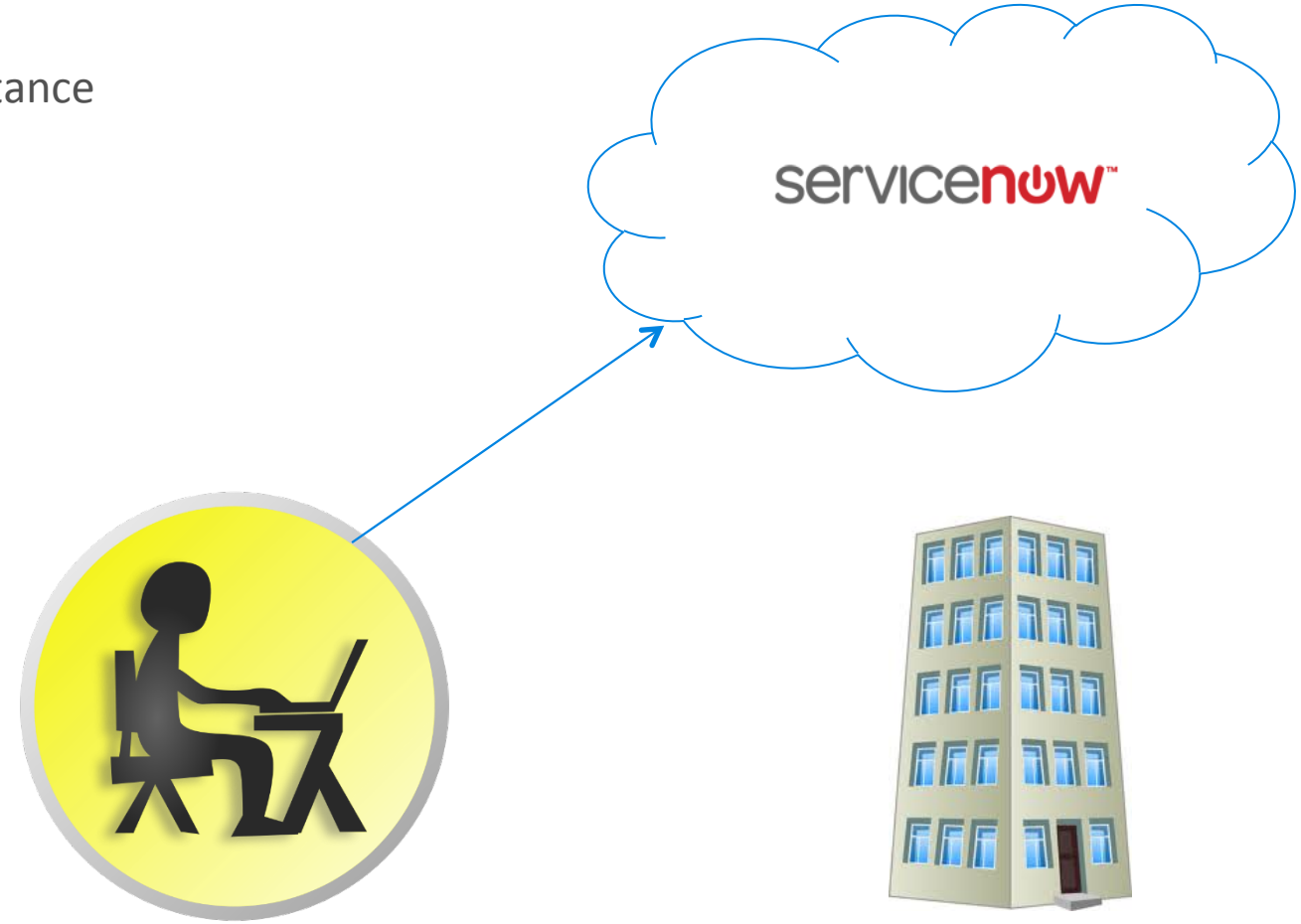
How SAML 2.0 Works

Service Provider Initiated Logon

© 2014 ServiceNow All Rights Reserved

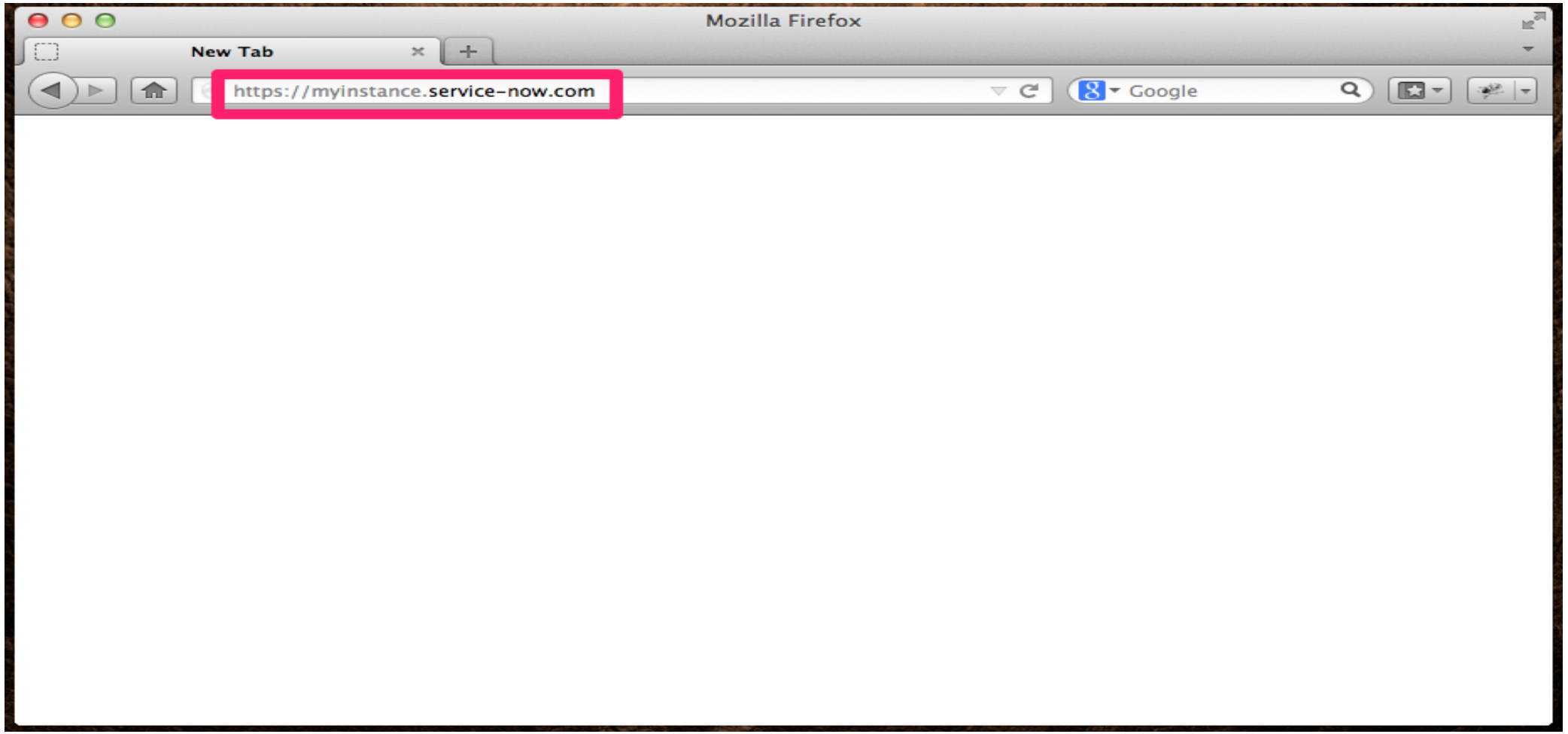
Service Provider Initiated Login

1. User attempts to browse to a ServiceNow instance



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

ServiceNow will..

1. Build an AuthnRequest XML document



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

```
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" AssertionConsumerServiceURL="https://
yourinstance.service-now.com/navpage.do" ForceAuthn="false" ID="SNCb7195eee1fd1b49083cc56cc0d14946d"
IsPassive="false" IssueInstant="2013-03-04T20:14:33.800Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" ProviderName="https://yourinstance.service-now.com/navpage.do" Version="2.0">

 <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://yourinstance.service-now.com</saml2:Issuer>

 <saml2p:NameIDPolicy AllowCreate="true" Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"/>

 <saml2p:RequestedAuthnContext Comparison="exact">

  <saml2:AuthnContextClassRef xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">urn:oasis:names:tc:SAML:
2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>

 </saml2p:RequestedAuthnContext>

</saml2p:AuthnRequest>
```

© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

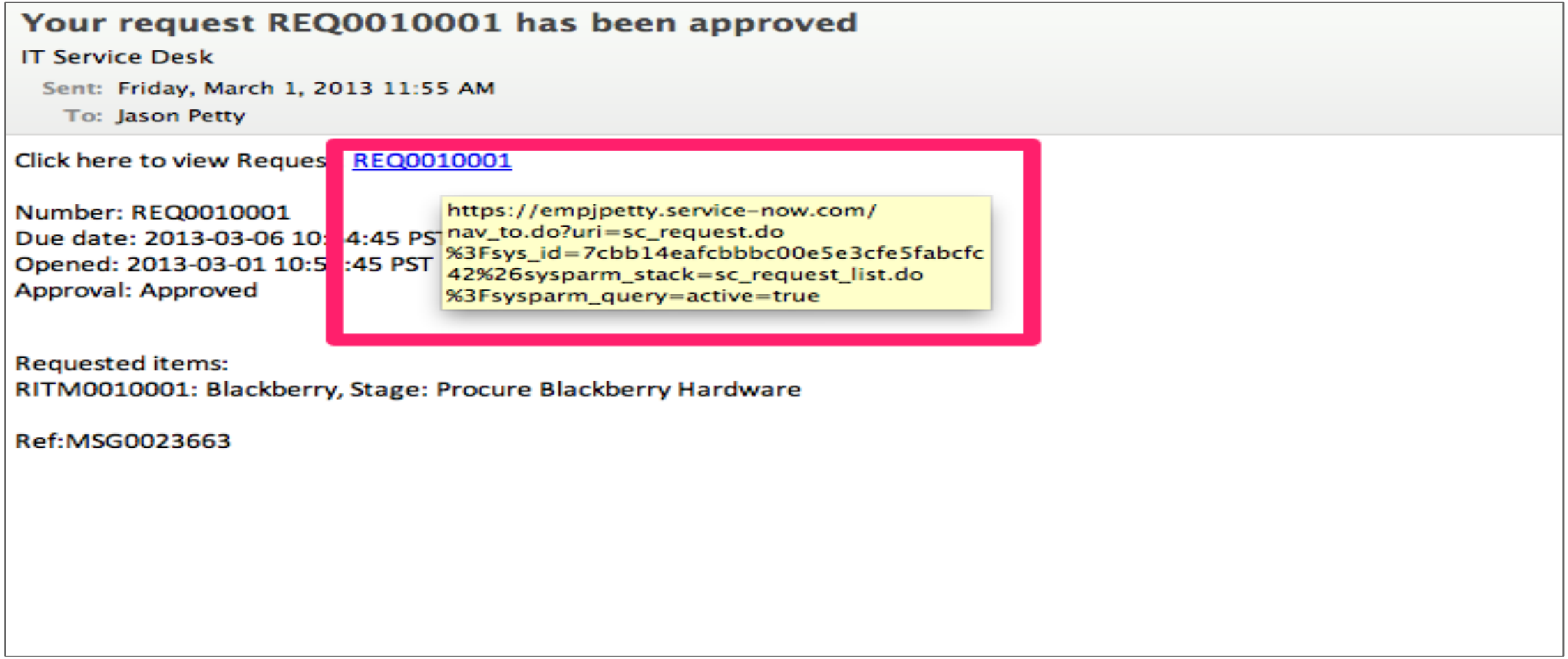
ServiceNow will..

1. Build an AuthnRequest XML document
2. Generate a RelayState



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

ServiceNow will…

1. Build an AuthnRequest XML Document
2. Generate a RelayState



- Default RelayState will be instance URL
  - RelayState = https://myinstance.service-now.com/navpage.do
- If a deep link is used in “nav_to.do” format, then that will be used as the Relay State instead
  - RelayState = https://myinstance.service-now.com/nav_to.do?uri=sc_request.do

© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

ServiceNow will…

1. Build an AuthnRequest XML Document
2. Generate a RelayState
3. Create encoded URL parameters for the AuthnRequest and RelayState
4. Tell client browser to redirect to the IdP URLwith the encoded URL parameters



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

ServiceNow tells the browser to redirect to the IdP with provided AuthnRequest and RelayState parameters

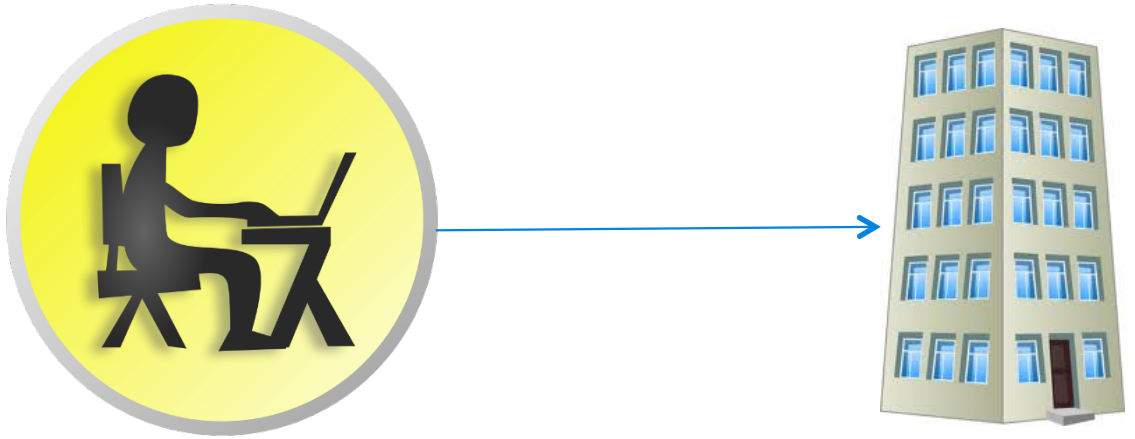


© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

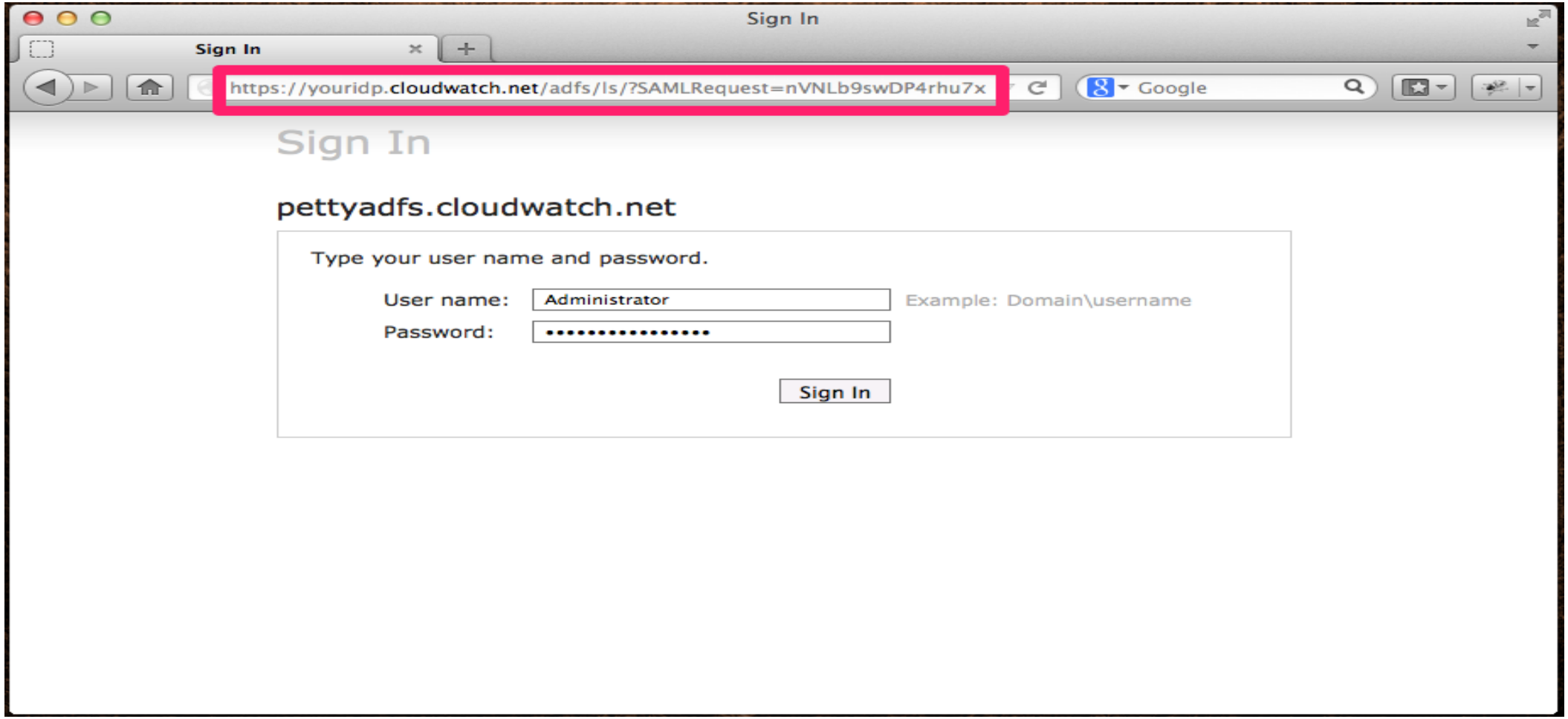
The browser then redirects to the URL and sends the encoded URL parameters provided by ServiceNow





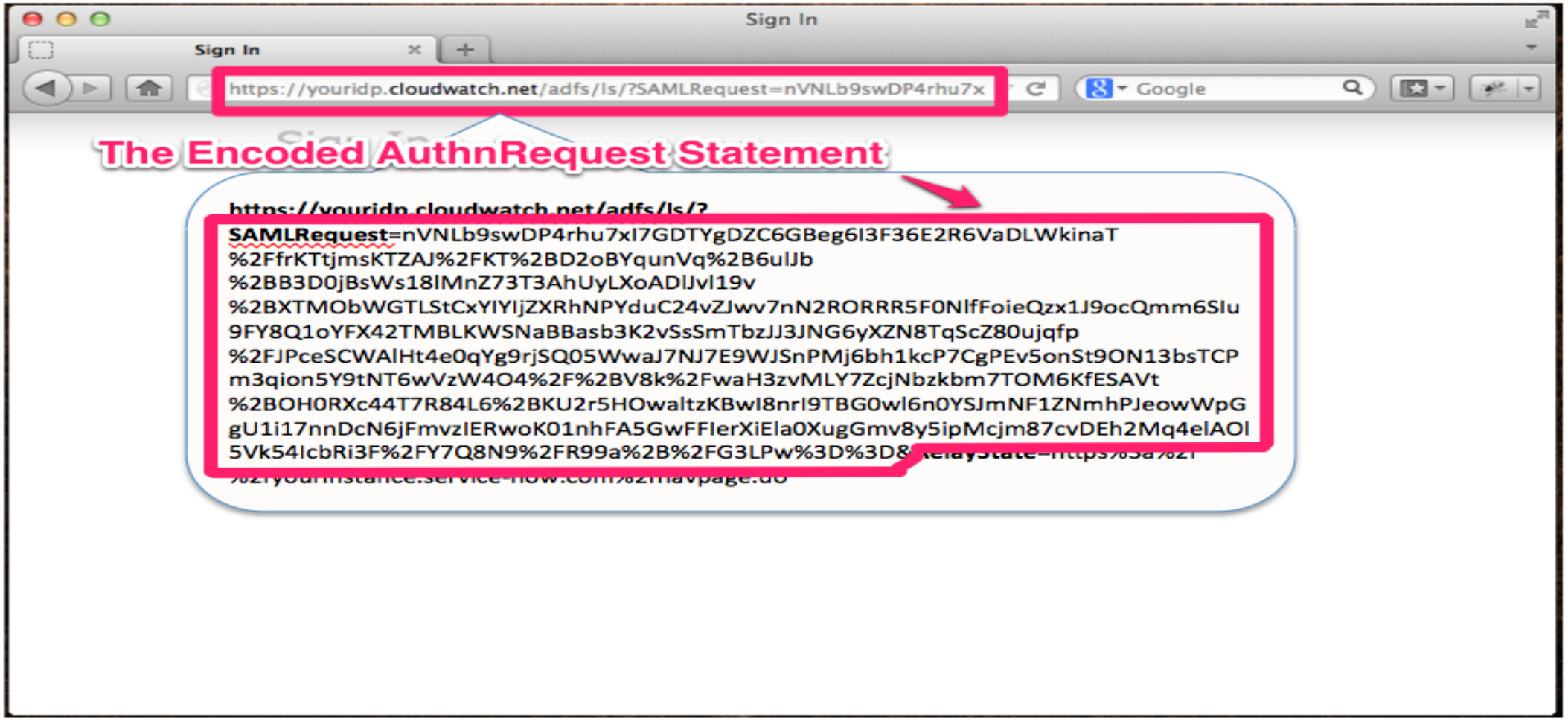
© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon



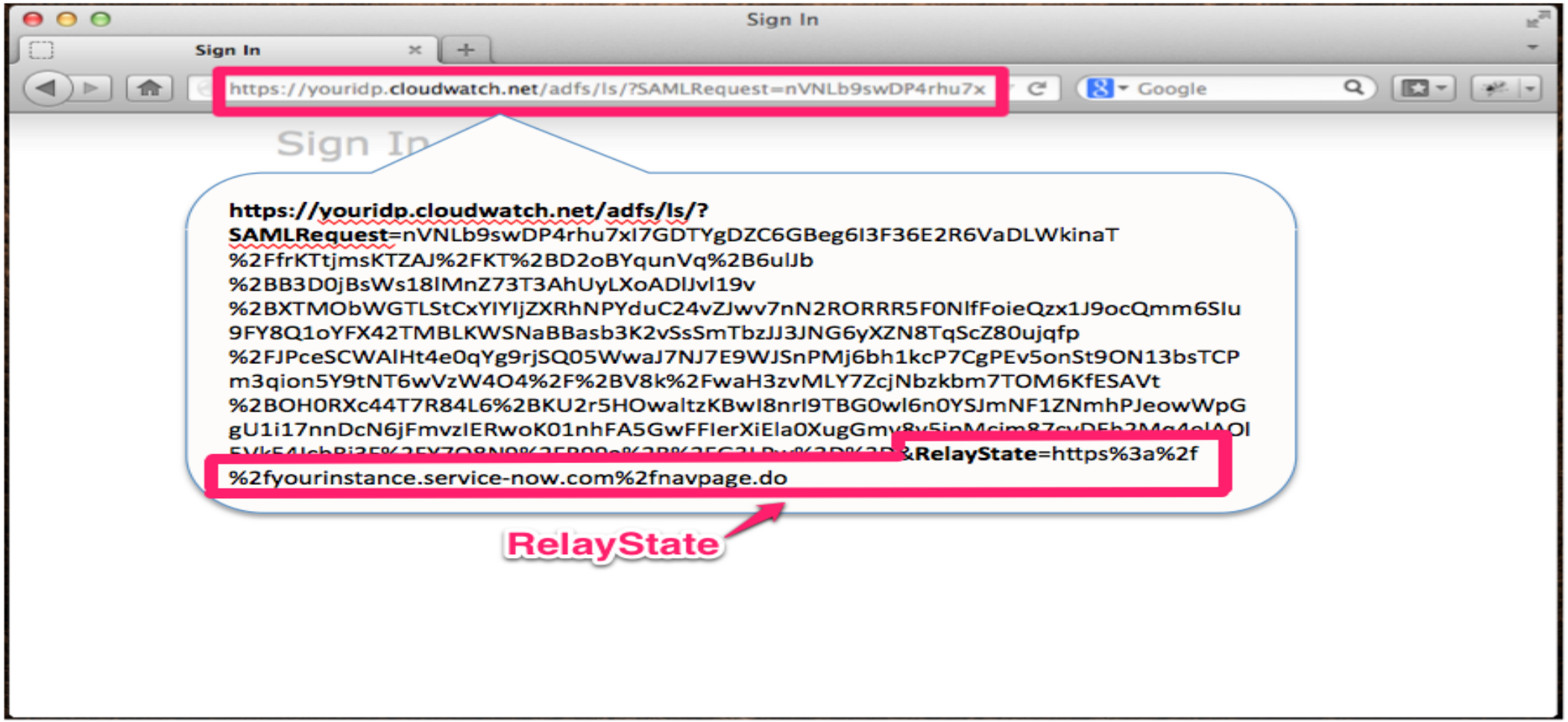
© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

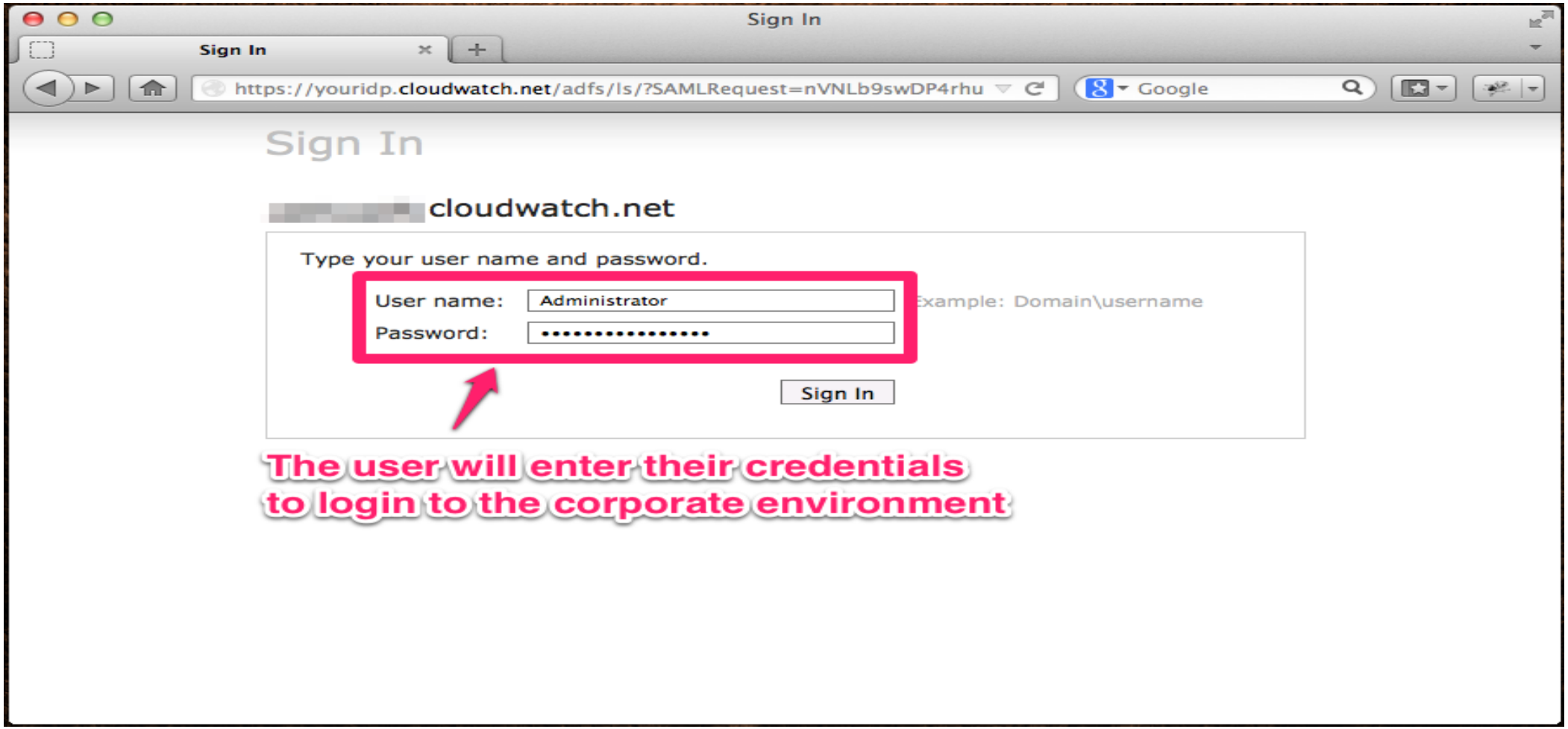


The Corporate Identity Provider (IdP) will then…

1. Decode the AuthnRequest statement
2. Save the RelayState for future use
3. Provide a login page for the user (if they do not already have an active session)

© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon



The Corporate Identity Provider (IdP) will then…

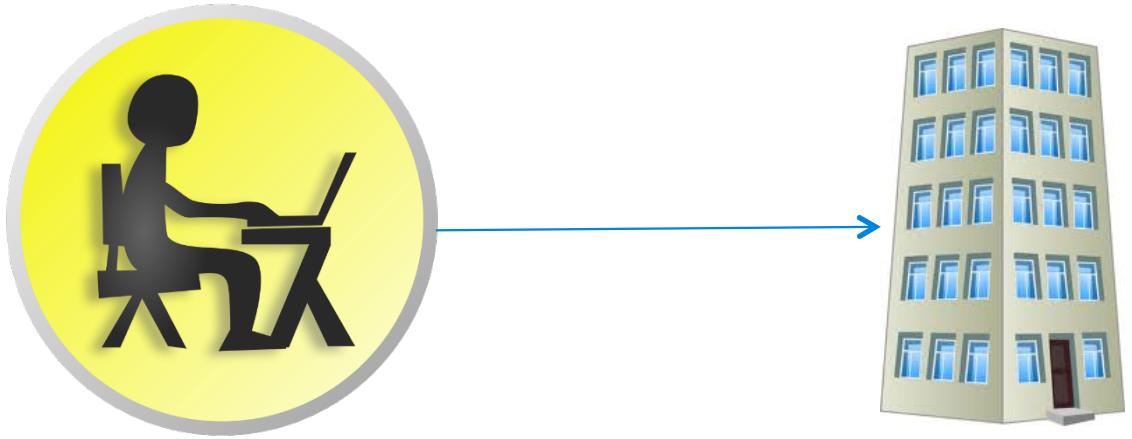
1. Decode the AuthnRequest statement
2. Save the RelayState for future use
3. Provide a login page for the user (if they do not already have an active session)
4. Tell the browser to redirect back to ServiceNow with the SAMLResponse and RelayState as POST parameters

© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

The IdP tells the browser to redirect back to ServiceNow with a form POST containing a SAMLResponse & RelayState

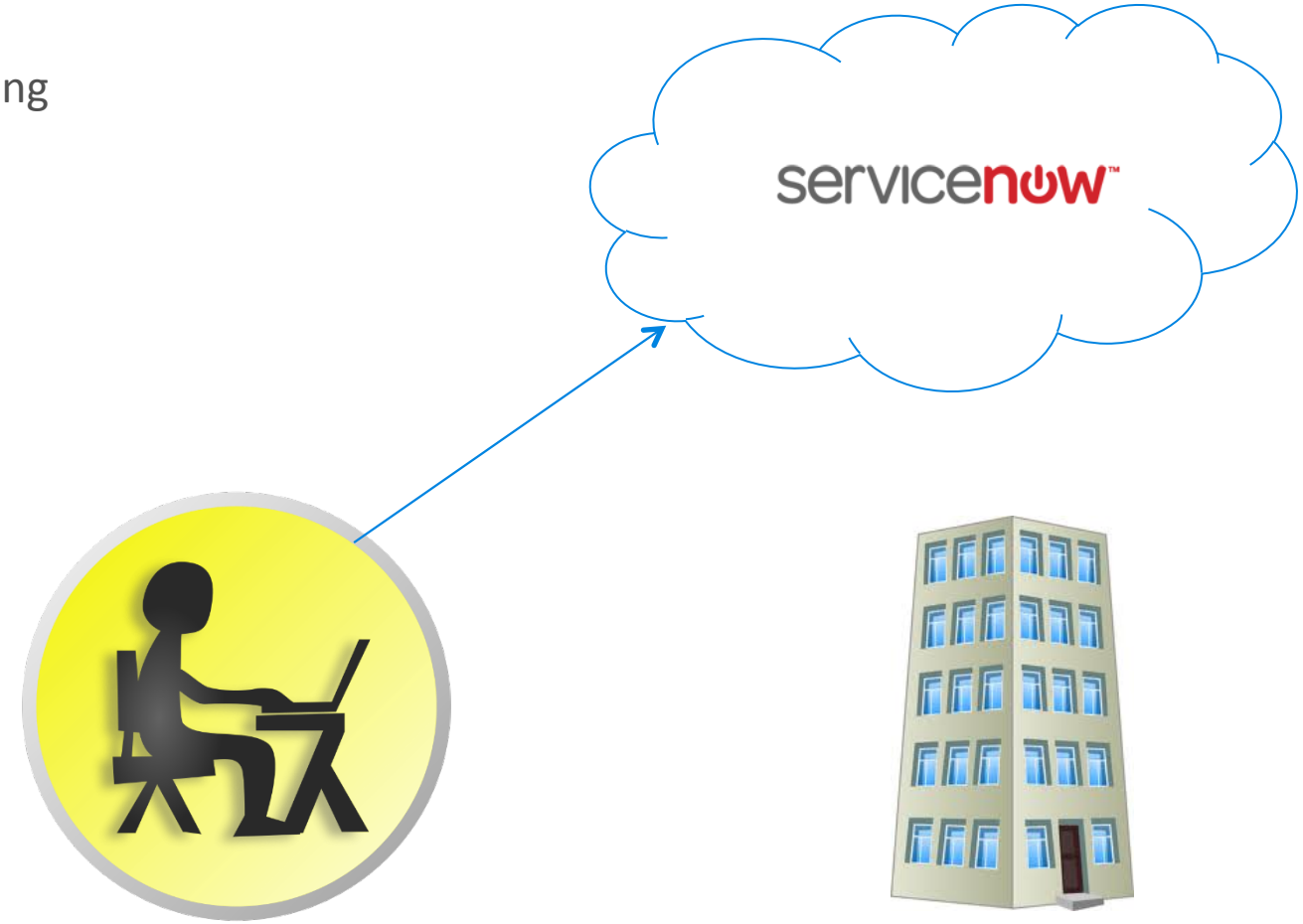




© 2014 ServiceNow All Rights Reserved

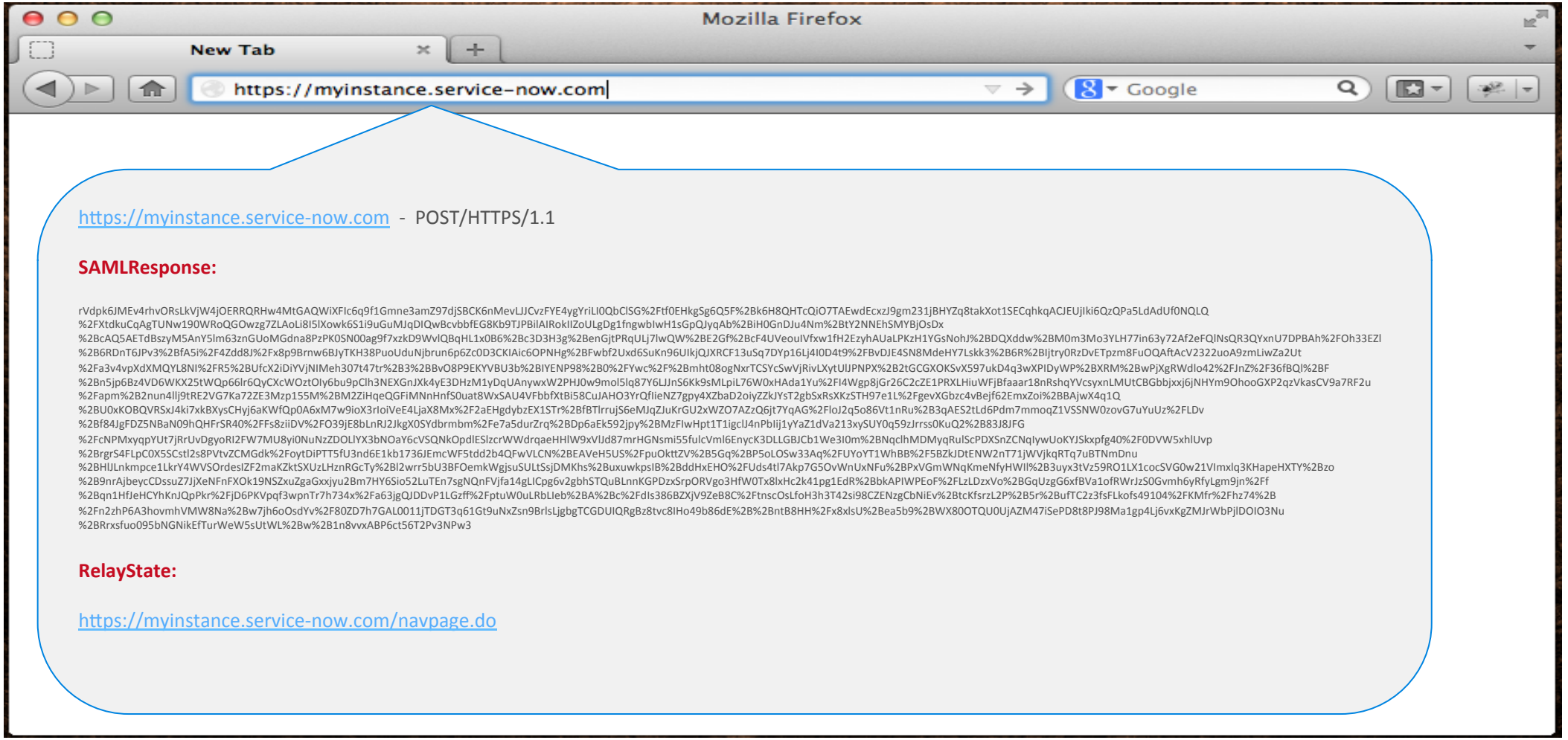
Service Provider Initiated Logon

The browser redirects to ServiceNow while POSTing the parameters from the IdP



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon



https://myinstance.service-now.com - POST/HTTPS/1.1

SAMLResponse:

rVdpk6JMEv4rhvORsLkVjW4jOERRQRHw4MtGAQWiXFIc6q9f1Gmne3amZ97djSBCK6nMevLJJCvzFYE4ygYriLI0QbClSG%2Ftf0EHkgSg6Q5F%2Bk6H8QHTcQiO7TAEwdEcxzJ9gm231jBHYZq8takXot1SECqhkqACJEUjIki6QzQPa5LdAdUf0NQLQ
%2FXtdkuCqAgTUNw190WRoQGOwzg7ZLAoLi8I5lXowk6S1i9uGuMJqDIQwBcvbbfEG8Kb9TJPBiIAIRokIIZoULgDg1fngwbIwH1sGpQJyqAb%2BiH0GnDJu4Nm%2BtY2NNEhSMYBjOsDx
%2BcAQ5AETdBszyM5AnY5lm63znGUoMGdna8PzPK0SN00ag9f7xzkD9WvlQBqHL1x0B6%2Bc3D3H3g%2BenGjtPRqULj7lwQW%2BE2Gf%2BcF4UVeouIVfxw1fH2EzyhAUaLPKzH1YGsNohJ%2BDQXddw%2BM0m3Mo3YLH77in63y72Af2eFQlNsQR3QYxnU7DPBAh%2FOh33EZl
%2B6RDnT6JPv3%2BfA5i%2F4Zdd8J%2Fx8p9Brnw6BJyTKH38PuoUduNjbrun6p6Zc0D3CKIAic6OPNHg%2BFwbf2Uxd6SuKn96UIkjQJXRCF13uSq7DYp16Lj4I0D4t9%2FBvDJE4SN8MdeHY7Lskk3%2B6R%2BIjtry0RzDvETpzm8FuOQAftAcV2322uoA9zmLiwZa2Ut
%2Fa3v4vpXdXMQYL8NI%2FR5%2BUfcX2iDiYVjNIMeh307t47tr%2B3%2BBvO8P9EKYVBU3b%2BIYENP98%2B0%2FYwc%2F%2Bmht08ogNxrTCSYcSwVjRivLXytUIJPNPX%2B2tGCGXOKSvX597ukD4q3wXPIDyWP%2BXRM%2BwPjXgRWdlo42%2FJnZ%2F36fBQl%2BF
%2Bn5jp6Bz4VD6WKX25tWQp66lr6QyCXcWOztOIy6bu9pClh3NEXGnJXk4yE3DHzM1yDqUAnywxW2PHJ0w9mol5lq87Y6LJJnS6Kk9sMLpiL76W0xHAda1Yu%2FI4Wgp8jGr26C2cZE1PRXLHiuWFjBfaaar18nRshqYvcsyxnLMUtCBGbbjxxj6jNHYm9OhooGXP2qzVkasCV9a7RF2u
%2Fapm%2B2nun4llj9tRE2VG7Ka72ZE3Mzp155M%2BM2ZiHqeQGFiMNnHnfS0uat8WxSAU4VFbbfXtBi58CuJAHO3YrQflieNZ7gpy4XZbaD2oiyZZkJYsT2gbSxRsXKzSTH97e1L%2FgevXGbzc4vBejf62EmxZoi%2BBAjwX4q1Q
%2BU0xKOBQVRSxJ4ki7xkBXysCHyj6aKWfQp0A6xM7w9ioX3rIoiVeE4LjaX8Mx%2F2aEHgdybzEX1STr%2BfBTlrrujS6eMJqZuKrGU2xWZO7AZzQ6jt7YqAG%2FloJ2q5o86Vt1nRu%2B3qAES2tLd6Pdm7mmoqZ1VSSNW0zovG7uYuUz%2FLDv
%2Bf84JgFDZ5NBaN09hQHFrSR40%2FFs8ziiDV%2FO39jE8bLnRJ2JkgX0SYdbrmbm%2Fe7a5durZrq%2BDp6aEk592jpy%2BMzFIwHpt1T1igcIJ4nPbIij1yYaZ1dVa213xySUY0q59zJrrss0KuQ2%2B83J8JFG
%2FcNPMxyqpYUt7jRrUvDgyoRI2FW7MU8yi0NuNzZDOLlYX3bNOaY6cVSQNkOpdlESlzcrWWdrqaeHHlW9xVlJd87mrHGNsmi55fulcVml6EnycK3DLLGBJCb1We3I0m%2BNqclhMDMyqRulScPDXSnZCNqIywUoKYJSkxpfg40%2F0DVW5xhlUvp
%2BrgrS4FLpC0X5SCstl2s8PVtvZCMGdk%2FoytDiPTT5fU3nd6E1kb1736JEmcWF5tdd2b4QFwVLCN%2BEAVeH5US%2FpuOkttZV%2B5Gq%2BP5oLOSw33Aq%2FUYoYT1WhBB%2F5BZkJDtENW2nT71jWVjkqRTq7uBTNmDnu
%2BHlJLnkmpce1LkrY4WVSOrdesIZF2maKZktSXUzLHznRGcTy%2Bl2wrr5bU3BFOemkWgjsuSULtSsjDMKhs%2BuxuwkpsIB%2BddHxEHO%2FUds4tl7Akp7G5OvWnUxNFu%2BPxVGmWNqKmeNfyHWIl%2B3uyx3tVz59RO1LX1cocSVG0w21VImxlq3KHapeHXTY%2Bzo
%2B9nrAjbeycCDssuZ7JjXeNFnFXOk19NSZxuZgaGxxjyu2Bm7HY6Sio52LuTEn7sgNQnFVjfa14gLICpg6v2gbhSTQuBLnnKGPDzxSrpORVgo3HfW0Tx8lxHc2k41pg1EdR%2BbkAPIWPEoF%2FLzLDzxVo%2BGqUzgG6xfBVa1ofRWrJzS0Gvmh6yRfyLgm9jn%2Ff
%2Bqn1HfJeHCYhKnJQpPkr%2FjD6PKVpqf3wpnTr7h734x%2Fa63jgQJDDvP1LGzff%2FptuW0uLRbLleb%2BA%2Bc%2FdIs386BZXjV9ZeB8C%2FtnscOsLfoH3h3T42si98CZENzgCbNiEv%2BtcKfsrzL2P%2B5r%2BufTC2z3fsFLkofs49104%2FKMfr%2Fhz74%2B
%2Fn2zhP6A3hovmhVMW8Na%2Bw7jh6oOsdYv%2F80ZD7h7GAL0011jTDGT3q61Gt9uNxZsn9BrlsLjgbgTCGDUIQRgBz8tvc8IHo49b86dE%2B%2BntB8HH%2Fx8xlsU%2Bea5b9%2BWX80OTQU0UjAZM47iSePD8t8PJ98Ma1gp4Lj6vxKgZMJrWbPjlDOIO3Nu
%2BRrxsfuo095bNGNikEfTurWeW5sUtWL%2Bw%2B1n8vvxABP6ct56T2Pv3NPw3

RelayState:

https://myinstance.service-now.com/navpage.do

© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

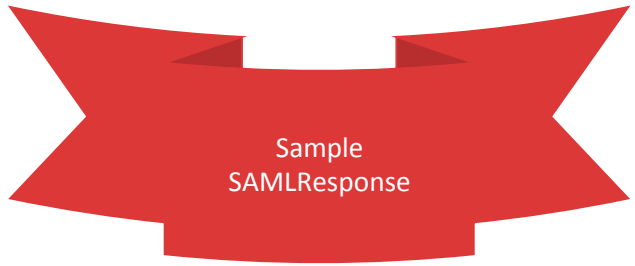
ServiceNow will…

1. Decode the SAMLResponse



© 2014 ServiceNow All Rights Reserved

```
<samlp:Response ID="_ebe10a33-21fb-4fa4-b085-400838854905" Version="2.0" IssueInstant="2013-03-05T16:29:32.429Z" Destination="https://yourinstance.service-now.com/navpage.do" Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
InResponseTo="SNCb014ba4cfabf8a401030357d180e6853"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
    <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">https://youridp.cloudwatch.net/adfs/services/trust</Issuer>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" /></samlp:Status>
    <Assertion ID="_b22ccfa0-44cc-4ada-8fef-c4c371beb915" IssueInstant="2013-03-05T16:29:32.429Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
        <Issuer>https://youridp.cloudwatch.net/adfs/services/trust</Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
                <ds:Reference URI="#_b22ccfa0-44cc-4ada-8fef-c4c371beb915">
                    <ds:Transforms>
                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /></ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                    <ds:DigestValue>6rl3gCVI4DSSmewIN0GXUrVT2DA49Q9V4BiF8buvcf8=</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>mOlUpEWfX1Yfr93ijwuihhnToExgf2rGF2QPXUFDp7MVDxagYv5ExJl8pJcXjpojxl0z3DZPHpTa8kpcpr8soa/HP+ZN5Gq+MkTnTxFzYSHNFTeb6MA0W+3v5yfNr3la/QNtVcFGlPBAmsw5kdObnV3JC1Y5Cuy1mONqJN7roGTiTUi84kuL52eUe
+2W8GWZxsombH3EkSsP7UWVMEcMacFQ60wuVfvw59orfx0P78Y2HIK0YJYKkATp3ocLH94G4mA/2sCgU4NHcL9NmtwfZCCgiCekNRXQXWeOf2e/aCEY5Xda1HbdUcRe8iXXtN7eQCT1t1UFFH3Z+nI+GtRopQ==</ds:SignatureValue>
            <KeyInfo
            xmlns="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>MIIC7DCCAdSgAwIBAgIQERQqiQ0aVq5K
+5l9udsU3DANBgkqhkiG9w0BAQsFADAyMTAwLgYDVQQDEydBREZTIFNpZ25pbmcgLSBwZXR0eWFkZnMuY2xvdWR3YXRjaC5uZXQwHhcNMTIxMDI1MTUxODAyWhcNMTMxMDI1MTUxODAyWjAyMTAwLgYDVQQDEydBREZTIFNpZ25pbmcgLSBwZXR0eWFkZnMuY2xvdWR3YXRjaC5uZXQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBA
QDBYTarOl+Uqzrc7L66Vc3wZwUtA3Jju1L6kdQOSpUI+A+K6q+gM8DikJ71v5k8ipN6Q5FZVAnynE35Qxr4lyhptFwidGPhx0smWcopf+2Uv51Fh/Svhtj4avCN5eXTuCrliUWGxlZ4ORU/7ZTUL+qR13asTbyPtlIL1RVDYQMndmvfU8zCFPArcNkm+XnO7fuczMeTdl/xHIeX4Pme0B7RuqcWNBfNL3FnS
+SvC2yv8FJSoYBpE2p0Uo00Kno0J2AmpQfj2uX/45MyqvjdRyt/B13ftuBIWX6pjzZUhBgL4FAx+RjETfoP2hfb7HFNGw7wqDD8CuzZMV7K/gabMaXlAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAIwCp/0vEO3gfjF4iSCZi5DW69UzoDkItoHzcy+SKb5xzjoUFKDoSz9DDNOqU2r+VV5SD1ZuosKInwyqnL+x3p28A/
hDZUrvP2LbBqQuTtBcGu10M6Dsd++eIW95YH5D5gFkboGks8AbwZr8PPeu1JmTRq9JJTslYkkqvNUNE2J/6Ufb0RFfh17Adv7fK2Y1QQMvTEDllY/ZMD0ZIXM8jvYri65mkLk77BY1Z+xnBY+nzx1WdzlOm6DqJfMm1/FtJSW/+4uXj8K5+qkBMxtLbJ1ZyYaeCKvGQVIda2Ug4wizNWs/nlGtBF7bIGSfpIUu2FRn
+GG9NWmmnkVlKDkVB4M=</ds:X509Certificate>
                </ds:X509Data>
                </KeyInfo>
        </ds:Signature>
        <Subject>
            <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">Administrator</NameID>
            <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <SubjectConfirmationData InResponseTo="SNCb014ba4cfabf8a401030357d180e6853" NotOnOrAfter="2013-03-05T16:34:32.429Z" Recipient="https://yourinstance.service-now.com/navpage.do" />
            </SubjectConfirmation>
        </Subject>
        <Conditions NotBefore="2013-03-05T16:29:32.422Z" NotOnOrAfter="2013-03-05T17:29:32.422Z">
            <AudienceRestriction>
                <Audience>https://yourinstance.service-now.com</Audience>
            </AudienceRestriction>
        </Conditions>
        <AttributeStatement>
            <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
                <AttributeValue>Administrator</AttributeValue>
            </Attribute>
        </AttributeStatement>
        <AuthnStatement AuthnInstant="2013-03-05T16:29:32.357Z" SessionIndex="_b22ccfa0-44cc-4ada-8fef-c4c371beb915">
            <AuthnContext>
                <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AuthnContextClassRef>
            </AuthnContext>
        </AuthnStatement>
    </Assertion>
</samlp:Response>
```

© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

ServiceNow will…

1. Decode the SAMLResponse
2. Validate security assertions



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
                <ds:Reference URI="#_b22ccfa0-44cc-4ada-8fef-c4c371beb915">
                    <ds:Transforms>
                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /></ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                    <ds:DigestValue>6rl3gCVI4DSSmewIN0GXUrVT2DA49Q9V4BiF8buvcf8=</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>mOlUpEWfX1Yfr93ijwuihhnToExgf2rGF2QPXUFDp7MVDxagYv5ExJl8pJcXjpojxl0z3DZPHpTa8kpcpr8soa/HP+ZN5Gq+MkTnTxFzYSHNFTeb6MA0W
+3v5yfNr3la/QNtVcFGlPBAmsw5kdObnV3JC1Y5Cuy1mONqJN7roGTiTUi84kuL52eUe+2W8GWZxsombH3EkSsP7UWVMEcMacFQ60wuVfvw59orfx0P78Y2HIK0YJYKkATp3ocLH94G4mA/
2sCgU4NHcL9NmtwfZCCgiCekNRXQXWeOf2e/aCEY5Xda1HbdUcRe8iXXtN7eQCT1t1UFFH3Z+nI+GtRopQ==</ds:SignatureValue>
            <KeyInfo
            xmlns="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>MIIC7DCCAdSgAwIBAgIQERQqiQ0aVq5K
+5l9udsU3DANBgkqhkiG9w0BAQsFADAyMTAwLgYDVQQDEydBREZTIFNpZ25pbmcgLSBwZXR0eWFkZnMuY2xvdWR3YXRjaC5uZXQwHhcNMTIxMDI1MTUxODAyWhcNMTMxMDI1MTUxODAyWjAyMTAwLgYD
VQQDEydBREZTIFNpZ25pbmcgLSBwZXR0eWFkZnMuY2xvdWR3YXRjaC5uZXQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDBYTarOl+Uqzrc7L66Vc3wZwUtA3Jju1L6kdQOSpUI+A+K6q
+gM8DikJ71v5k8ipN6Q5FZVAnynE35Qxr4lyhptFwidGPhx0smWcopf+2Uv51Fh/Svhtj4avCN5eXTuCrliUWGxlZ4ORU/7ZTUL+qR13asTbyPtlIL1RVDYQMndmvfU8zCFPArcNkm
+XnO7fuczMeTdl/xHIeX4Pme0B7RuqcWNBfNL3FnS+SvC2yv8FJSoYBpE2p0Uo00Kno0J2AmpQfj2uX/45MyqvjdRyt/B13ftuBIWX6pjzZUhBgL4FAx+RjETfoP2hfb7HFNGw7wqDD8CuzZMV7K/
gabMaXlAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAIwCp/0vEO3gfjF4iSCZi5DW69UzoDkItoHzcy+SKb5xzjoUFKDoSz9DDNOqU2r+VV5SD1ZuosKInwyqnL+x3p28A/
hDZUrvP2LbBqQuTtBcGu10M6Dsd++eIW95YH5D5gFkboGks8AbwZr8PPeu1JmTRq9JJTslYkkqvNUNE2J/6Ufb0RFfh17Adv7fK2Y1QQMvTEDllY/ZMD0ZIXM8jvYri65mkLk77BY1Z+xnBY
+nzx1WdzlOm6DqJfMm1/FtJSW/+4uXj8K5+qkBMxtLbJ1ZyYaeCKvGQVIda2Ug4wizNWs/nlGtBF7bIGSfpIUu2FRn+GG9NWmmnkVlKDkVB4M=</ds:X509Certificate>
                </ds:X509Data>
                </KeyInfo>
        </ds:Signature>
```

Security information in SAMLResponse

© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

ServiceNow will…

1. Decode the SAMLResponse
2. Validate security assertions
3. Look for the NameID token



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

```
<Subject>
            <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">youremail@domain.com</NameID>
            <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <SubjectConfirmationData InResponseTo="SNCb014ba4cfabf8a401030357d180e6853" NotOnOrAfter="2013-03-05T16:34:32.429Z"
Recipient="https://yourinstance.service-now.com/navpage.do" />
            </SubjectConfirmation>
        </Subject>
```



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

ServiceNow will…

1. Decode the SAMLResponse
2. Validate security assertions
3. Look for the NameID token
4. Match the token with a user in the sys_user table



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

```
<Subject>
        <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">itam@yourcompany.com<
NameID>
        <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm  arer">
          <SubjectConfirmationData InResponseTo="SNCb014ba4cfabf  030357d180e6853"
NotOnOrAfter="2013-03-05T16:34:32.429Z" Recipient="https://yourins  ce.service-now.com/navpage.do" />
        </SubjectConfirmation>
      </Subject>
```

Match NameID token with appropriate field in sys_user table

User ID	Name		
antione.mccleary	Antione Mccleary		tru
antony.thierauf	Antony Thierauf		tru
approver	Approver User	approver ample.com	tru
armando.kolm	Armando Kolm	armand @example.com	tru
armando.papik	Armando Papik	armando. pik@example.com	tru
ashley.leonesio	Ashley Leonesio	ashley.leonesio@example.com	tru
itam	Asset Manager	itam@example.com	tru
athena.fontanilla	Athena Fontanilla	athena.fontanilla@example.com	tru
audra.cantu	Audra Cantu	audra.cantu@example.com	tru
avery.parbol	Avery Parbol	avery.parbol@example.com	tru
barbara.hindley	Barbara Hindley	barbara.hindley@example.com	tru
bart.hachey	Bart Hachey	bart.hachey@example.com	tru

© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon

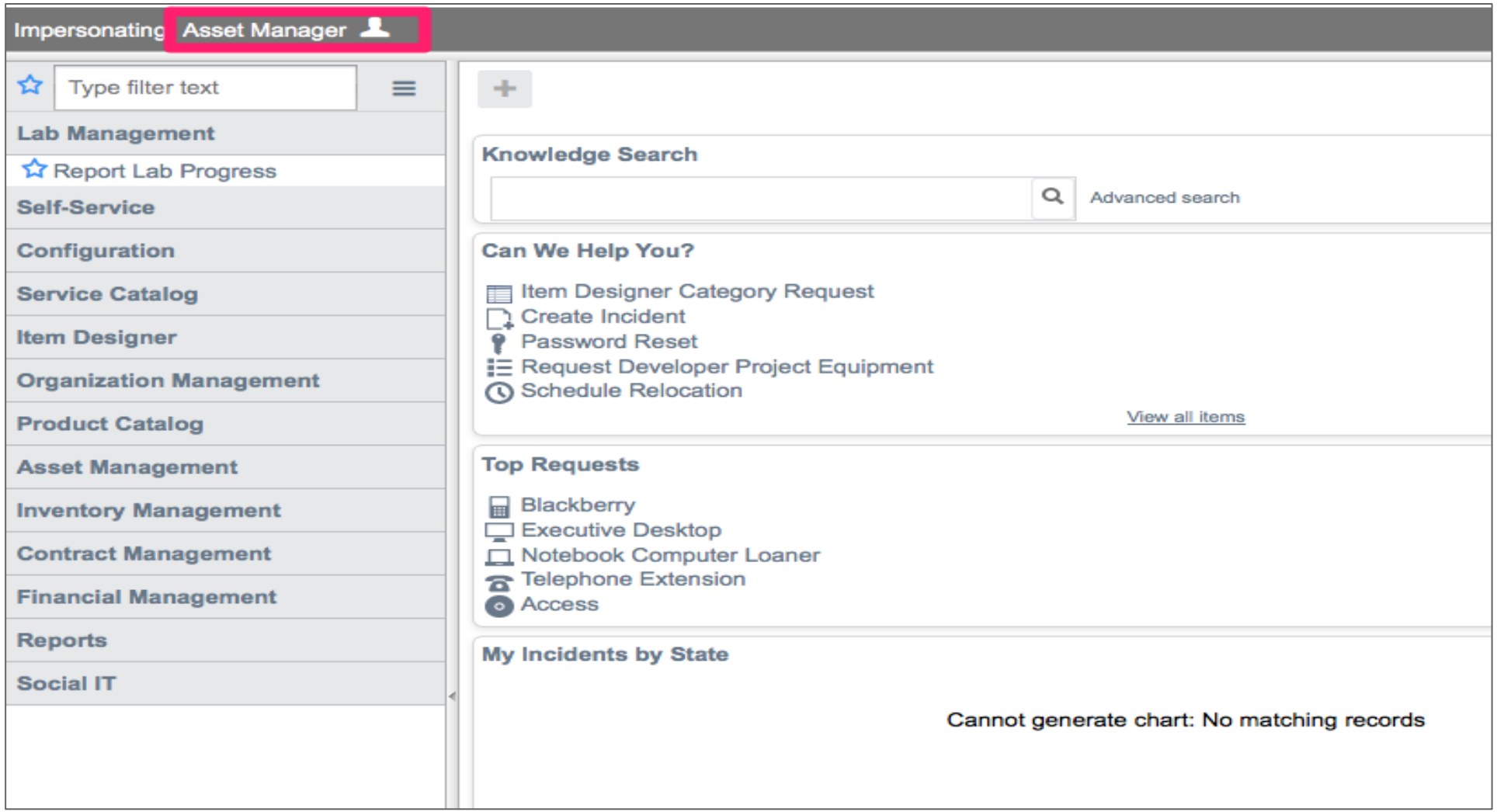
ServiceNow will…

1. Decode the SAMLResponse
2. Validate security assertions
3. Look for the NameID token
4. Match the token with a user in the sys_user table
5. Authenticate as that user



© 2014 ServiceNow All Rights Reserved

Service Provider Initiated Logon



© 2014 ServiceNow All Rights Reserved

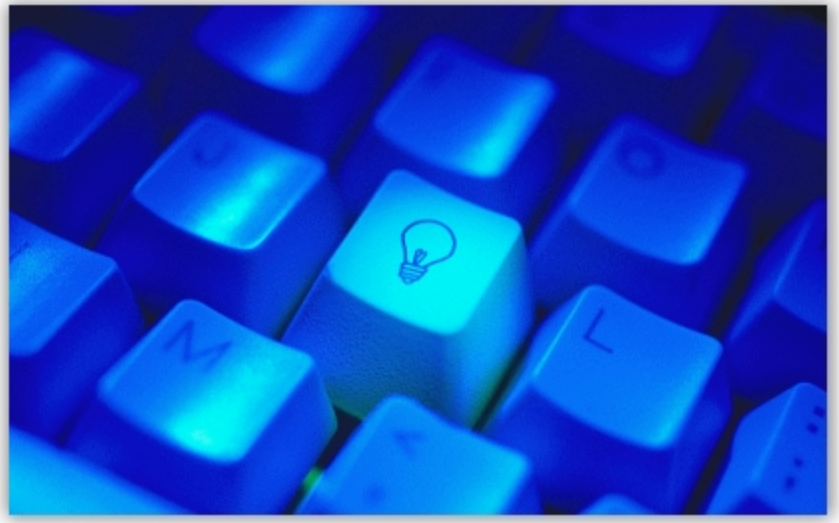
Service Provider Initiated Logon

ServiceNow will…

1. Decode the SAMLResponse
2. Validate security assertions
3. Look for the NameID token
4. Match the token with a user in the sys_user table
5. Authenticate as that user
6. Redirect to the URL specified in the RelayState parameter



© 2014 ServiceNow All Rights Reserved



Hands-On Lab #1

Setup temporary email and
SSO Circle account

© 2014 ServiceNow All Rights Reserved

How SAML 2.0 Works

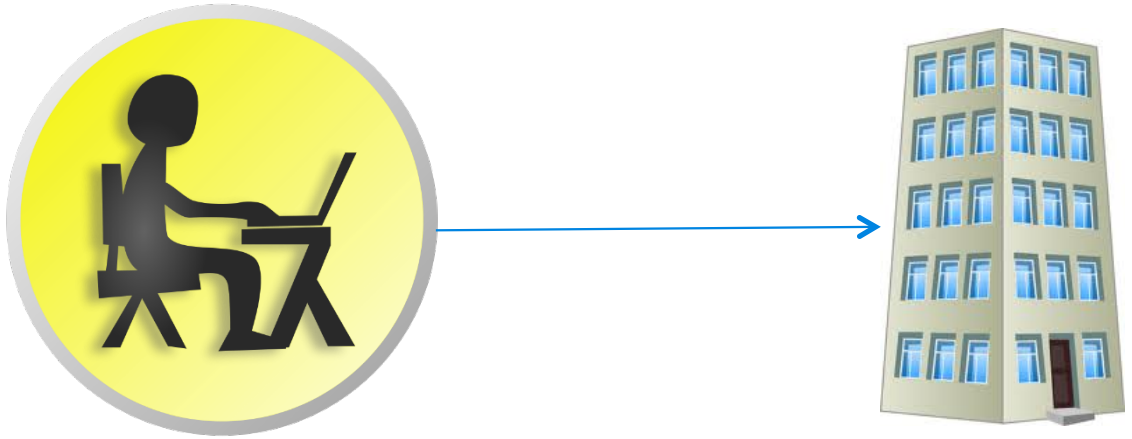
Identity Provider Initiated Logon

© 2014 ServiceNow All Rights Reserved

Identity Provider Initiated Logon

The user logs into the company portal and then choses to go to ServiceNow from the Portal





© 2014 ServiceNow All Rights Reserved

Identity Provider Initiated Logon



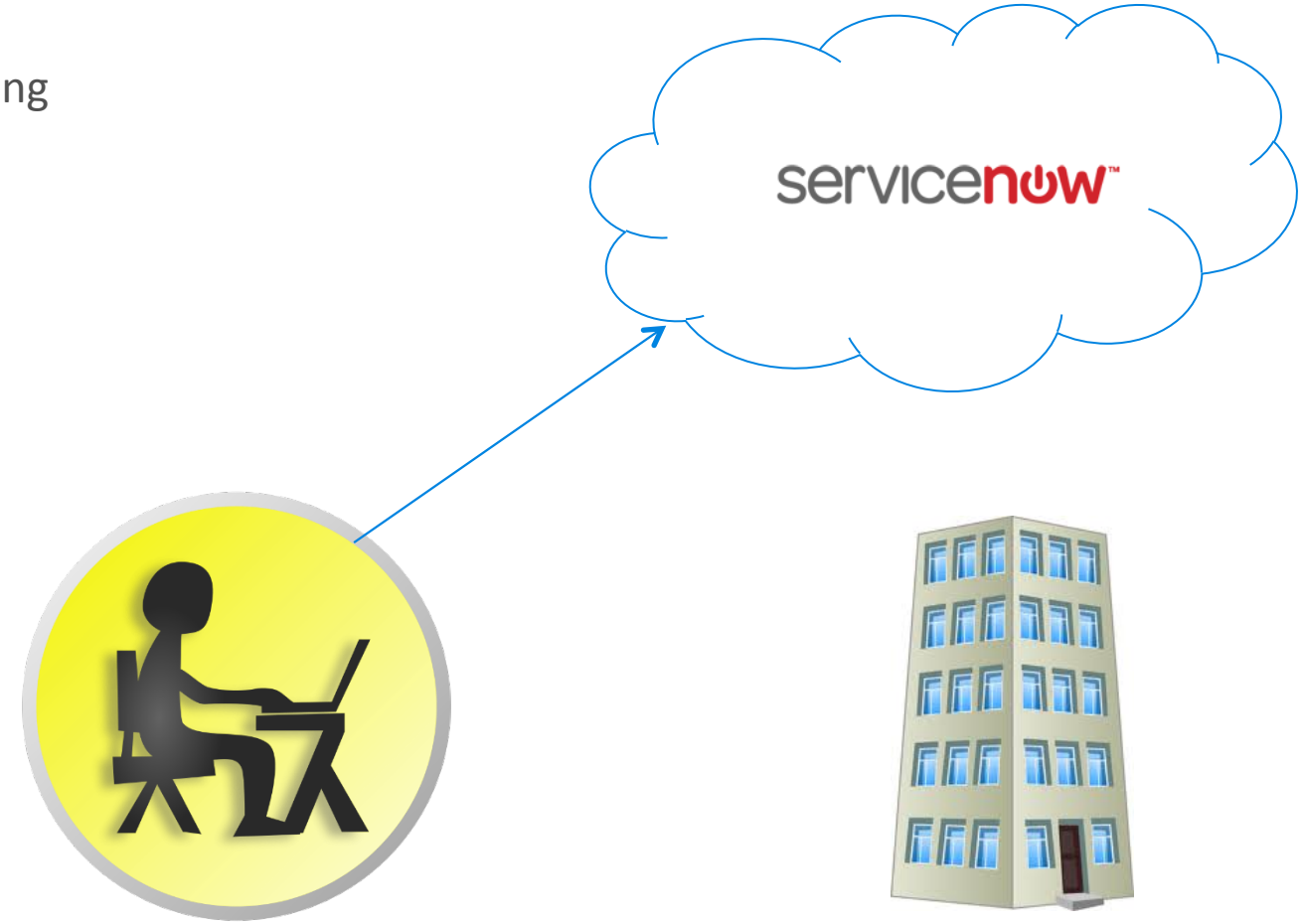
The Corporate portal will then…

1. Build and encode an XML-based SAML Response Document
2. Tell the browser to redirect back to ServiceNow with the SAMLResponse as a POST parameter

© 2014 ServiceNow All Rights Reserved

Identity Provider Initiated Logon

The browser redirects to ServiceNow while POSTing the parameter from the IDP



© 2014 ServiceNow All Rights Reserved

Identity Provider Initiated Logon

ServiceNow will…

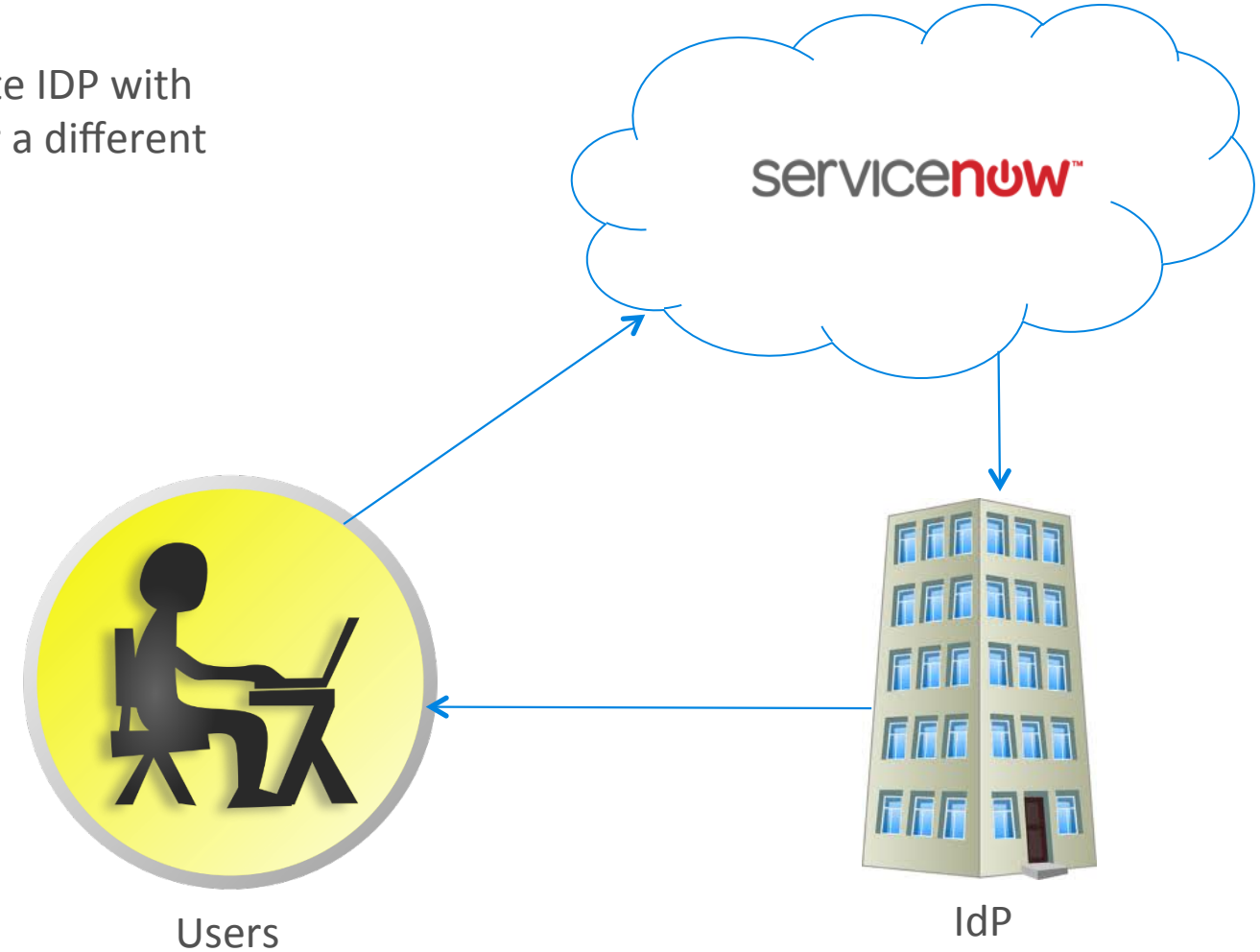
1. Decode the SAMLResponse
2. Validate security assertions
3. Look for the NameID token
4. Match the token with a user in the sys_user table
5. Authenticate as that user



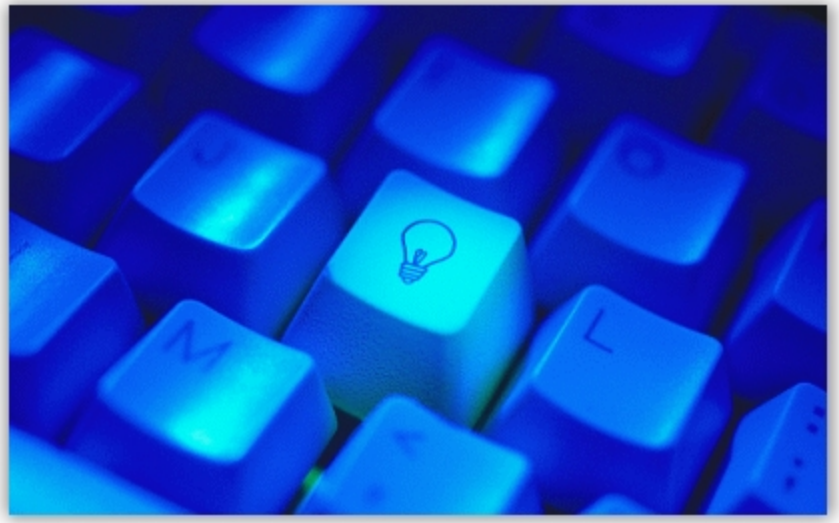
© 2014 ServiceNow All Rights Reserved

Identity Provider Initiated Logon

You have now successfully linked up the corporate IDP with ServiceNow and users will not have to remember a different login.



© 2014 ServiceNow All Rights Reserved



Hands-On Lab #2

Setup your own SAML 2.0 Authentication

© 2014 ServiceNow All Rights Reserved

Tools

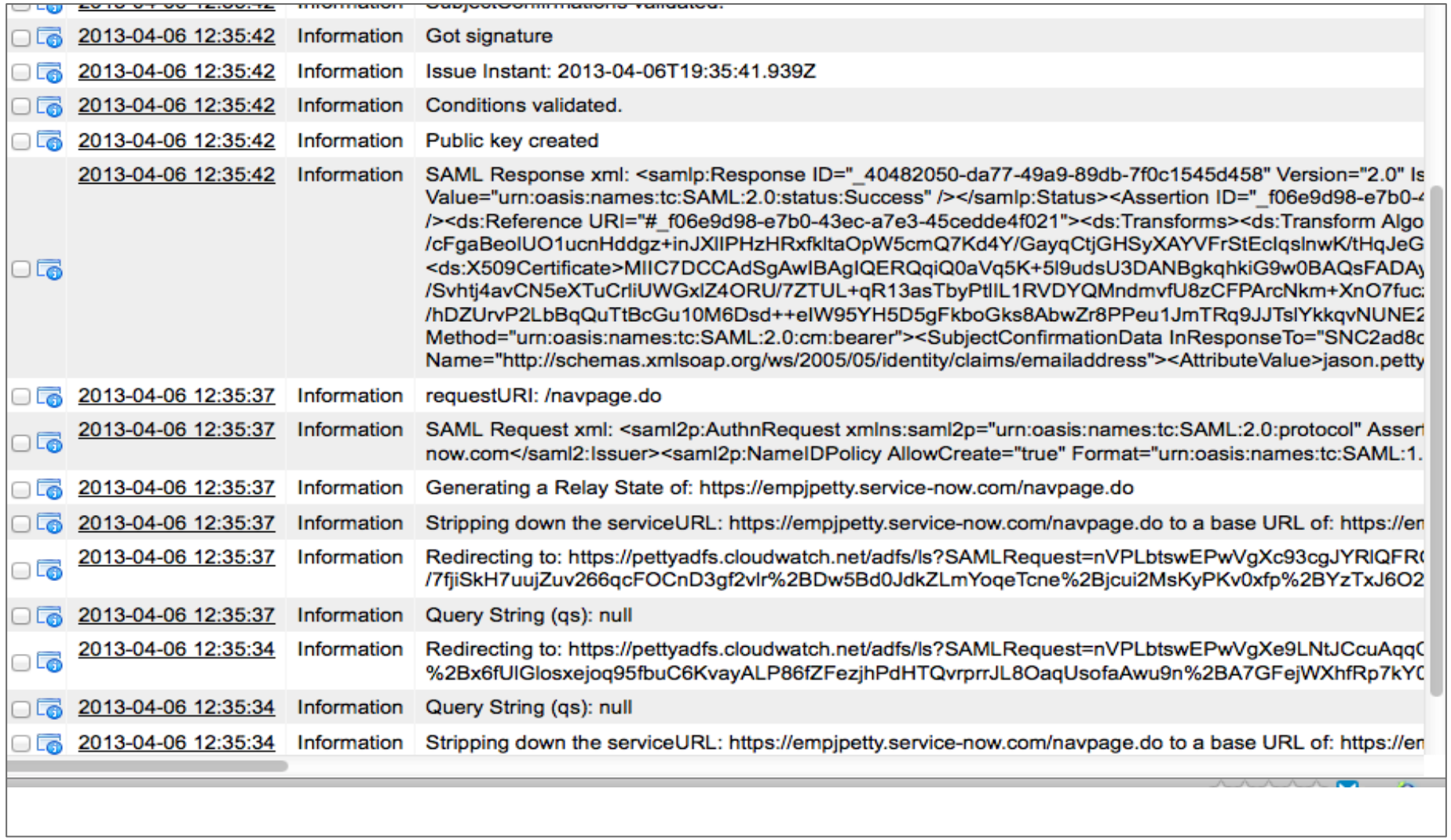
© 2014 ServiceNow All Rights Reserved

Tools for SAML

- Logs in ServiceNow Instance (Can be turned on and off)
- SAML 2.0 Encoder/Decoder
  - https://rnd.feide.no/simplesaml/module.php/saml2debug/debug.php
- Trace with Chrome
  - View > Developer > Developer Tools
- Trace with Firefox
  - Tools > Web Developer > Web Console
- Tracing with Fiddler
  - http://www.fiddler2.com/fiddler2/

© 2014 ServiceNow All Rights Reserved

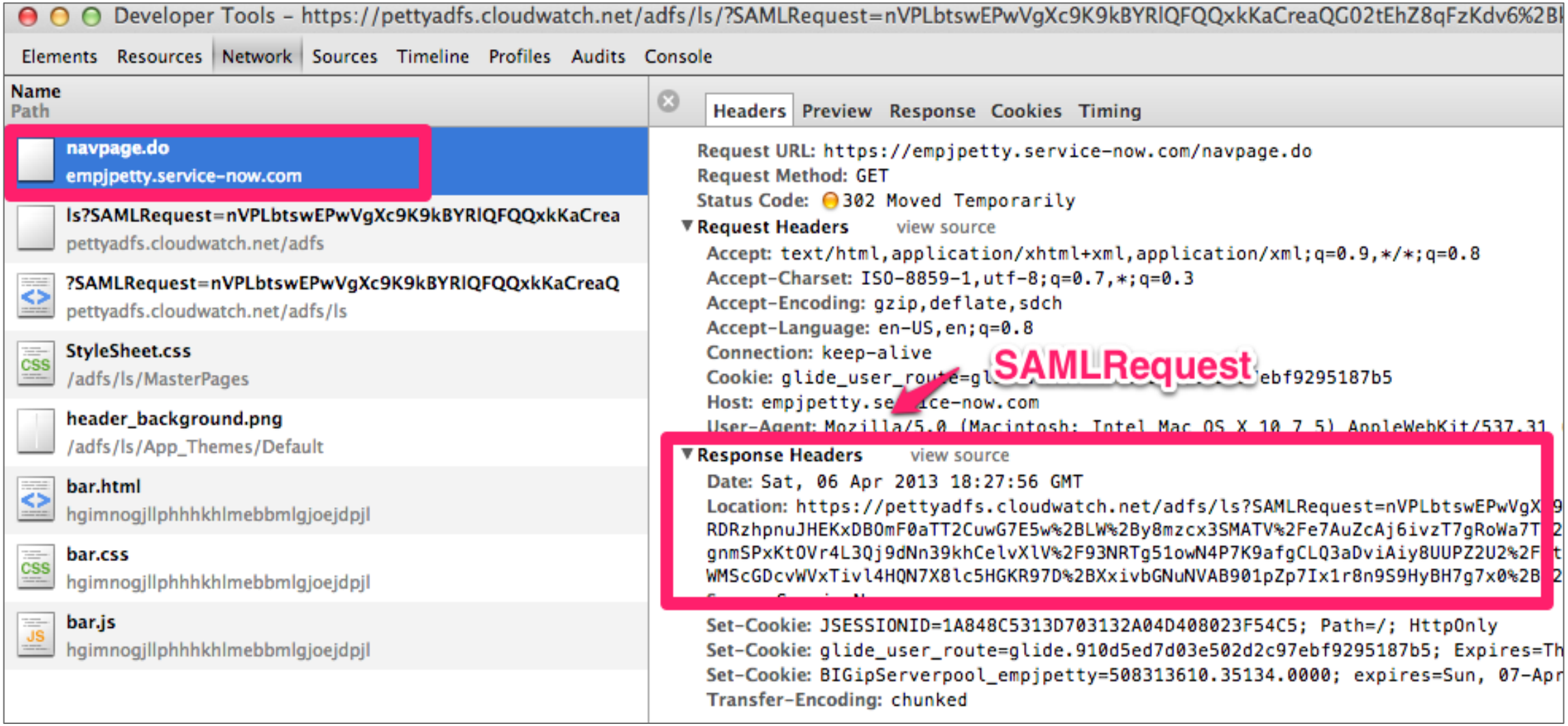
Logs in ServiceNow Instance



2013-04-06 12:35:42	Information	Got signature
2013-04-06 12:35:42	Information	Issue Instant: 2013-04-06T19:35:41.939Z
2013-04-06 12:35:42	Information	Conditions validated.
2013-04-06 12:35:42	Information	Public key created
2013-04-06 12:35:42	Information	SAML Response xml: <samlp:Response ID="_40482050-da77-49a9-89db-7f0c1545d458" Version="2.0" Is Value="urn:oasis:names:tc:SAML:2.0:status:Success" /></samlp:Status><Assertion ID="_f06e9d98-e7b0- /><ds:Reference URI="#_f06e9d98-e7b0-43ec-a7e3-45cedde4f021"><ds:Transforms><ds:Transform Algo /cFgaBeolUO1ucnHddgz+inJXIIPHzHRxfkltaOpW5cmQ7Kd4Y/GayqCtjGHSyXAYVFrStEclqslnwK/tHqJeG <ds:X509Certificate>MIIC7DCCAdSgAwIBAgIQERQqiQ0aVq5K+5l9udsU3DANBgkqhkiG9w0BAQsFADA /Svhtj4avCN5eXTuCrliUWGxlZ4ORU/7ZTUL+qR13asTbyPtlIL1RVDYQMndmvfU8zCFPArcNkm+XnO7fuc /hDZUrvP2LbBqQuTtBcGu10M6Dsd++elW95YH5D5gFkboGks8AbwZr8PPeu1JmTRq9JJTslYkkqvNUNE2 Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><SubjectConfirmationData InResponseTo="SNC2ad8c Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"><AttributeValue>jason.petty
2013-04-06 12:35:37	Information	requestURI: /navpage.do
2013-04-06 12:35:37	Information	SAML Request xml: <saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" Assert now.com</saml2:Issuer><saml2p:NameIDPolicy AllowCreate="true" Format="urn:oasis:names:tc:SAML:1.
2013-04-06 12:35:37	Information	Generating a Relay State of: https://empjpetty.service-now.com/navpage.do
2013-04-06 12:35:37	Information	Stripping down the serviceURL: https://empjpetty.service-now.com/navpage.do to a base URL of: https://en
2013-04-06 12:35:37	Information	Redirecting to: https://pettyadfs.cloudwatch.net/adfs/ls?SAMLRequest=nVPLbtswEPwVgXc93cgJYRlQFR /7fjiSkH7uujZuv266qcFOCnD3gf2vlr%2BDw5Bd0JdkZLmYoqeTcne%2Bjcui2MsKyPKv0xfp%2BYzTxJ6O2
2013-04-06 12:35:37	Information	Query String (qs): null
2013-04-06 12:35:34	Information	Redirecting to: https://pettyadfs.cloudwatch.net/adfs/ls?SAMLRequest=nVPLbtswEPwVgXe9LNtJCcuAqq %2Bx6fUlGlosxejoq95fbuC6KvayALP86fZFezjhPdHTQvrprrJL8OaqUsofaAwu9n%2BA7GFejWXhfRp7kY
2013-04-06 12:35:34	Information	Query String (qs): null
2013-04-06 12:35:34	Information	Stripping down the serviceURL: https://empjpetty.service-now.com/navpage.do to a base URL of: https://en

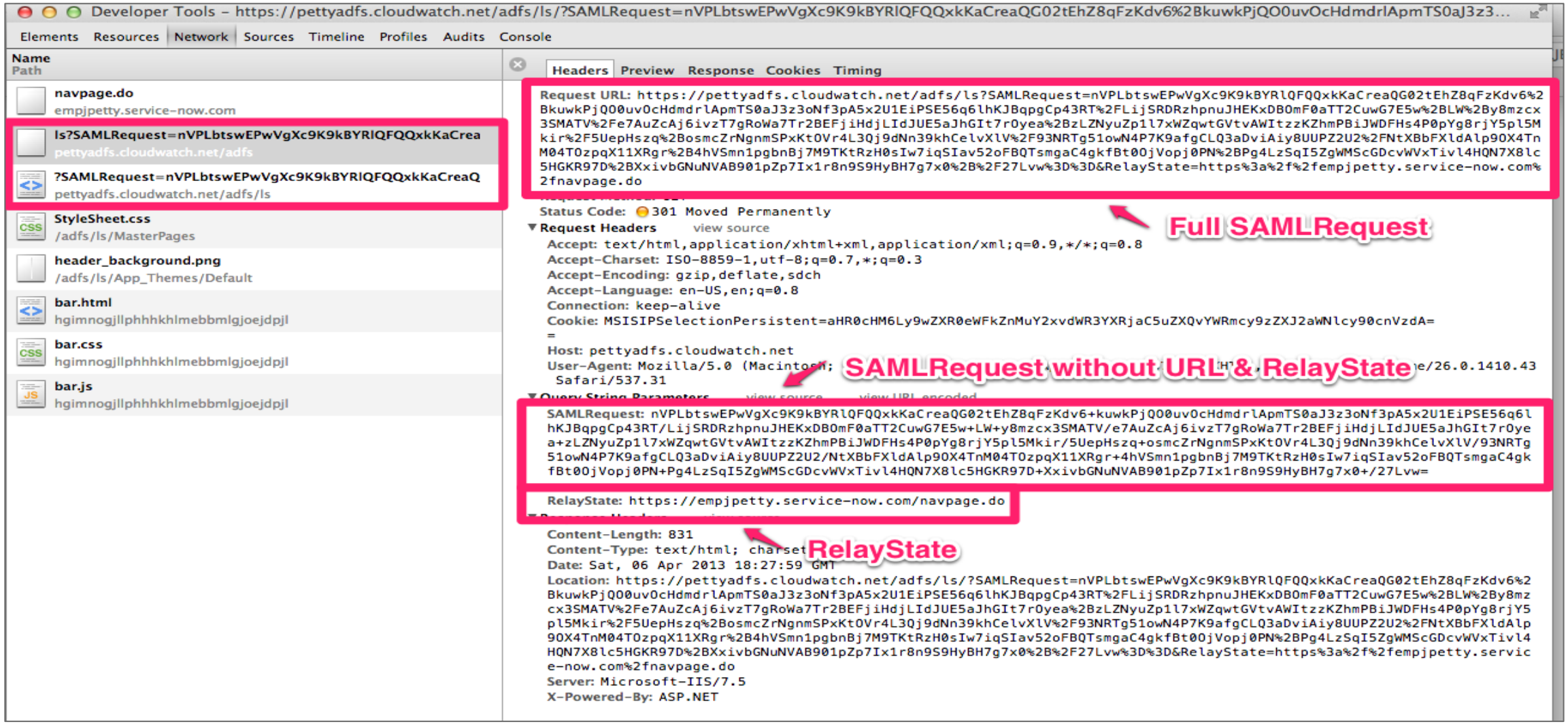
© 2014 ServiceNow All Rights Reserved

Tracing In Chrome



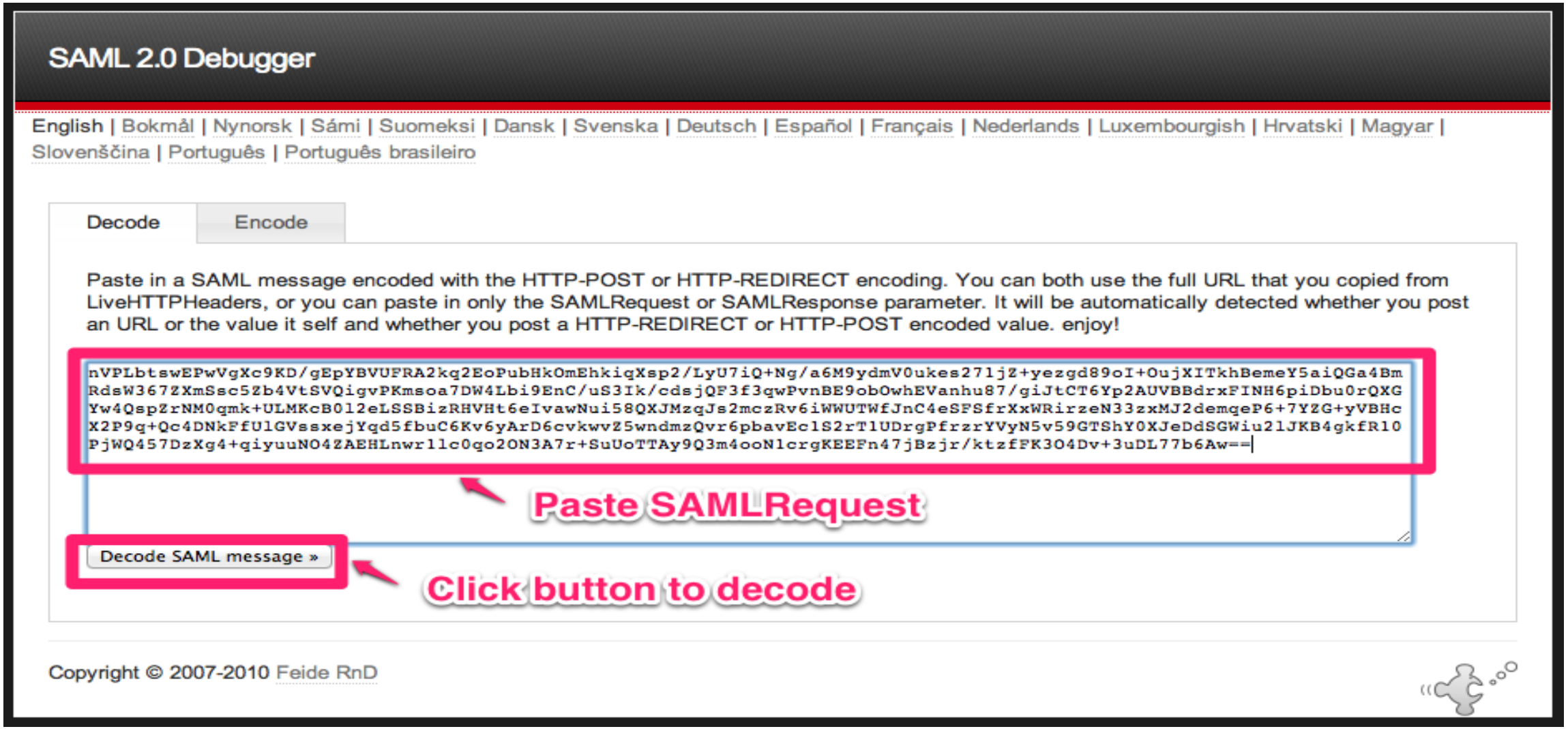
© 2014 ServiceNow All Rights Reserved

Tracing In Chrome



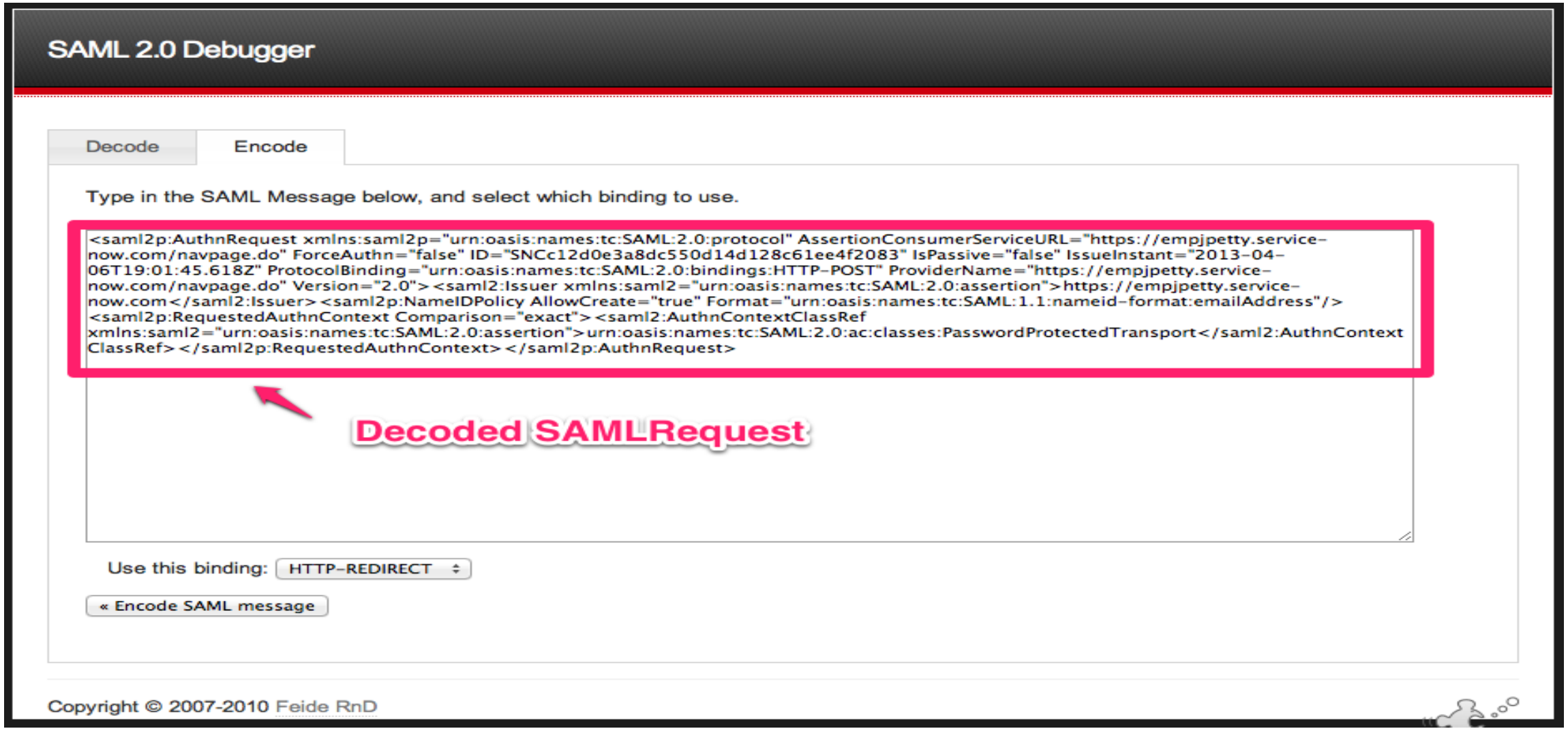
© 2014 ServiceNow All Rights Reserved

Tracing In Chrome



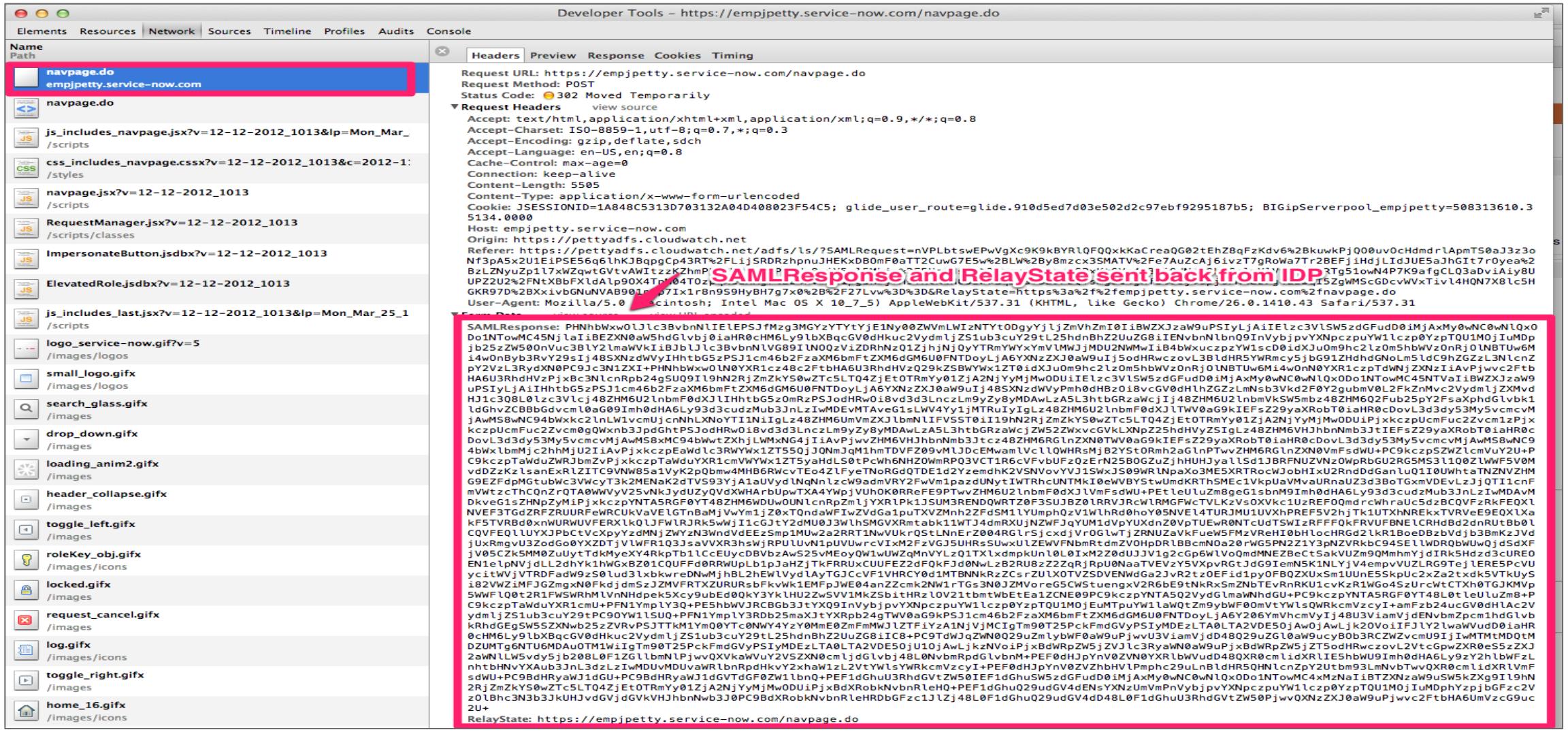
© 2014 ServiceNow All Rights Reserved

Tracing In Chrome



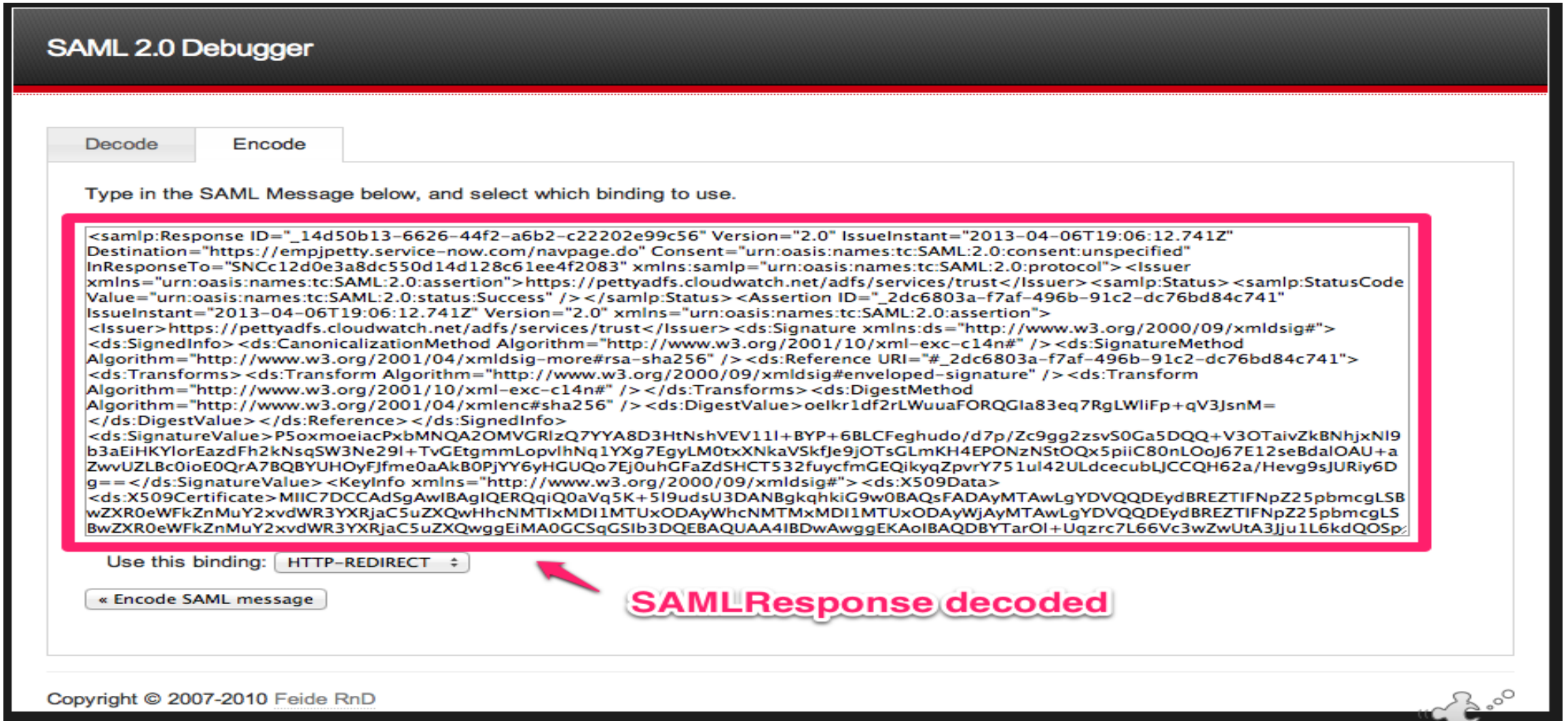
© 2014 ServiceNow All Rights Reserved

Tracing In Chrome



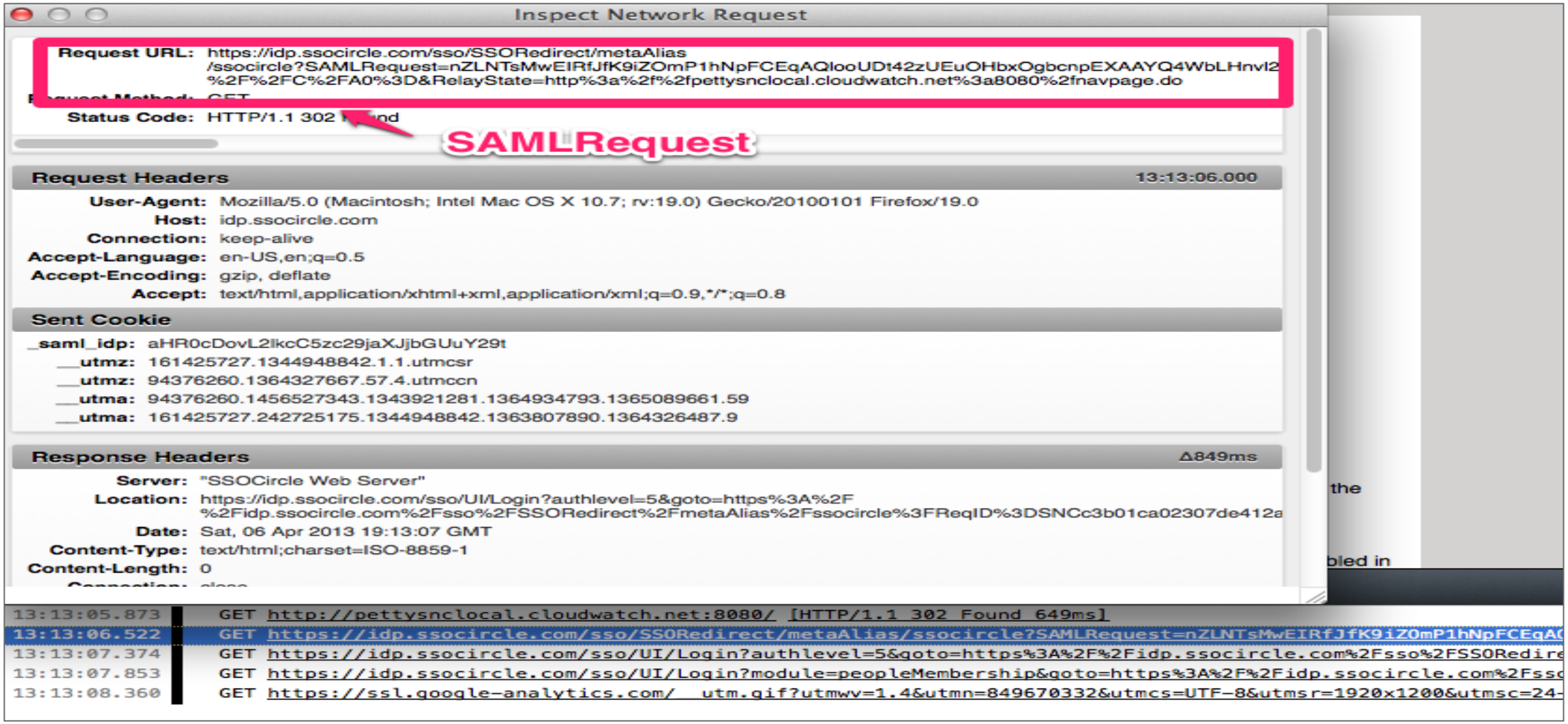
© 2014 ServiceNow All Rights Reserved

Tracing In Chrome



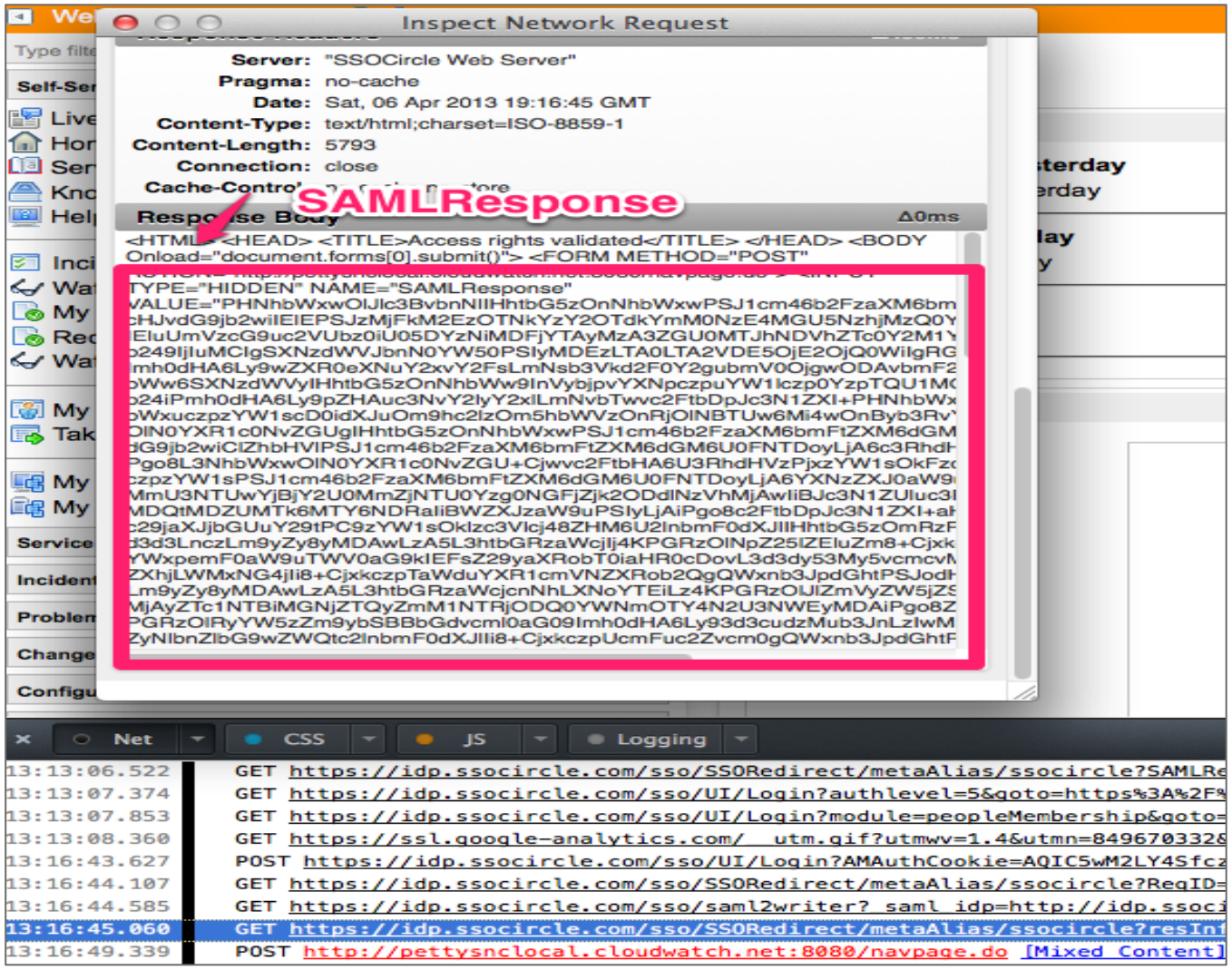
© 2014 ServiceNow All Rights Reserved

Tracing In Firefox



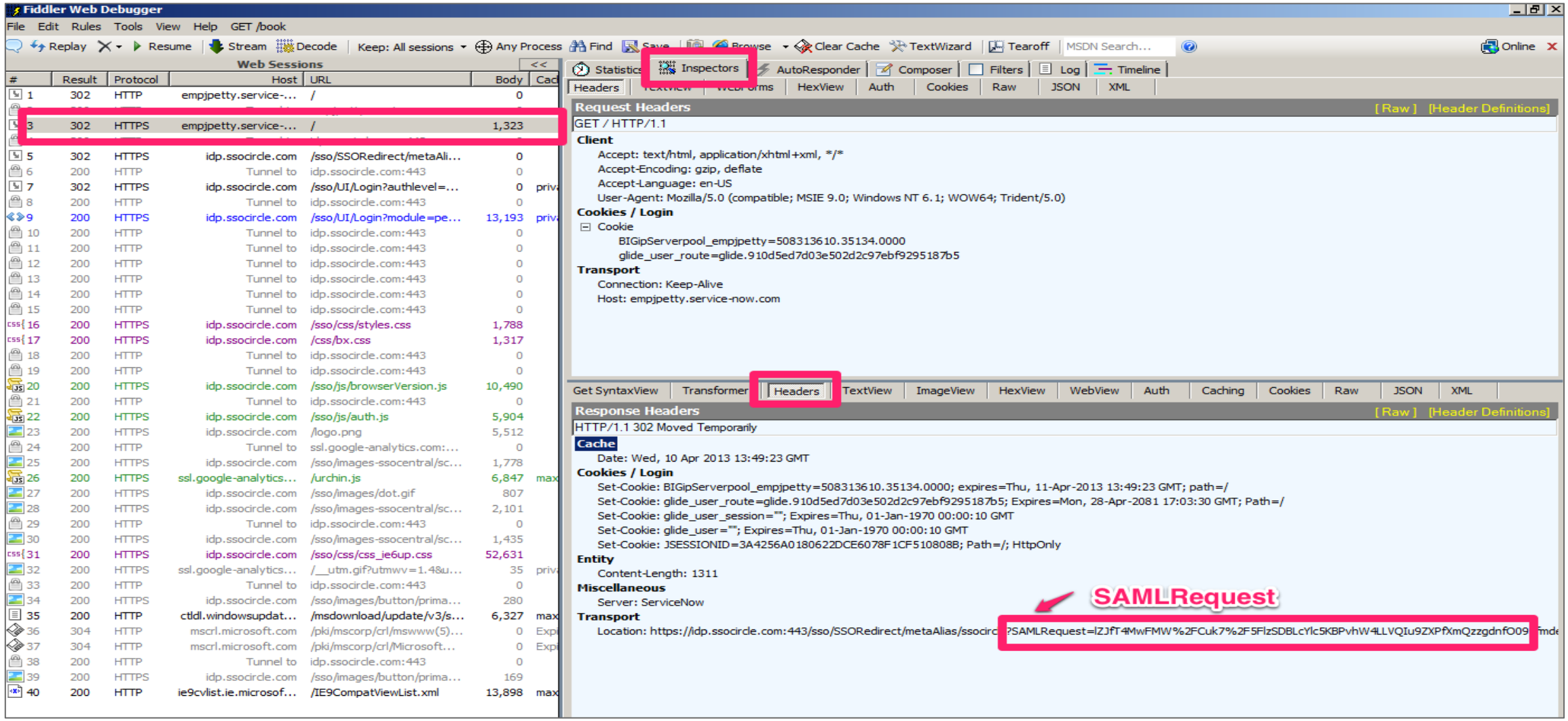
© 2014 ServiceNow All Rights Reserved

Tracing In Firefox



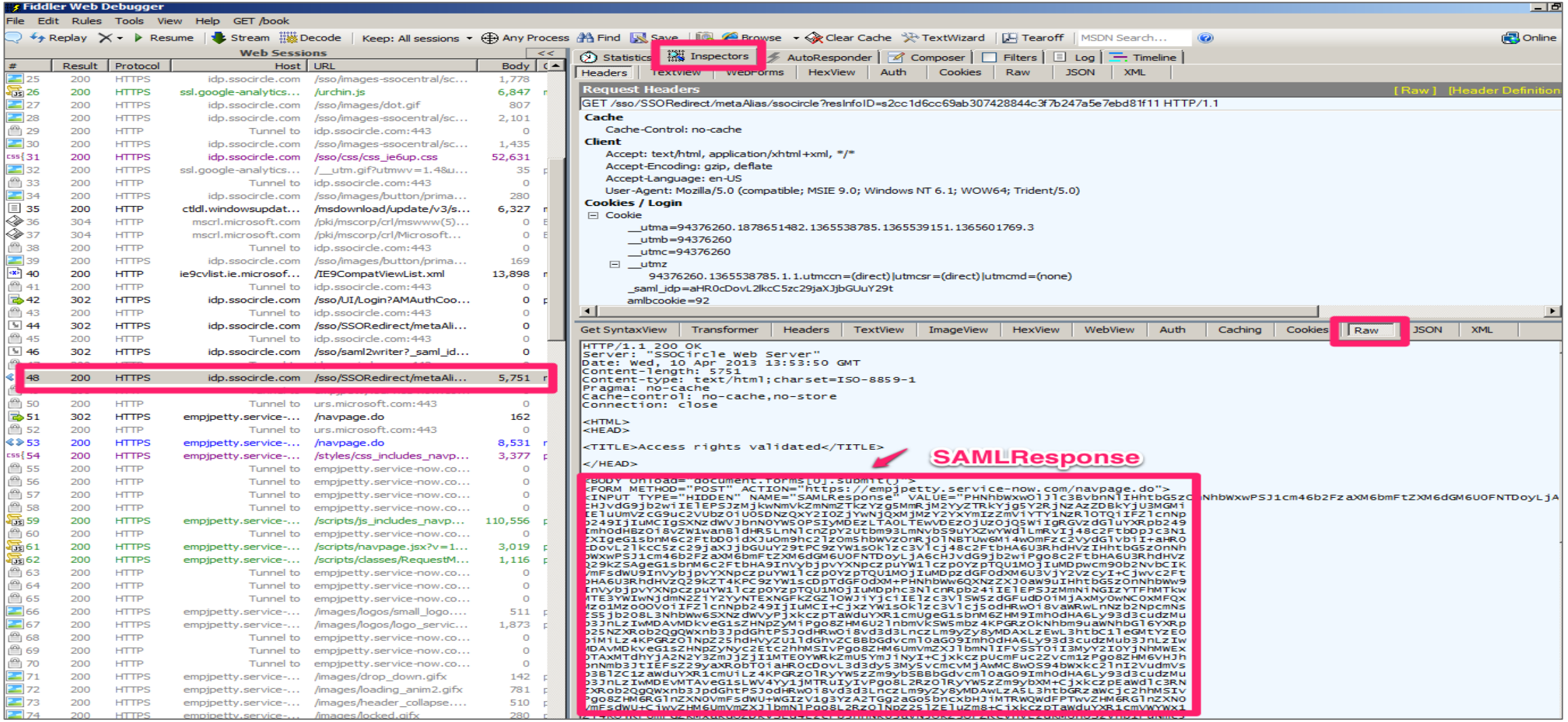
© 2014 ServiceNow All Rights Reserved

Tracing In Fiddler

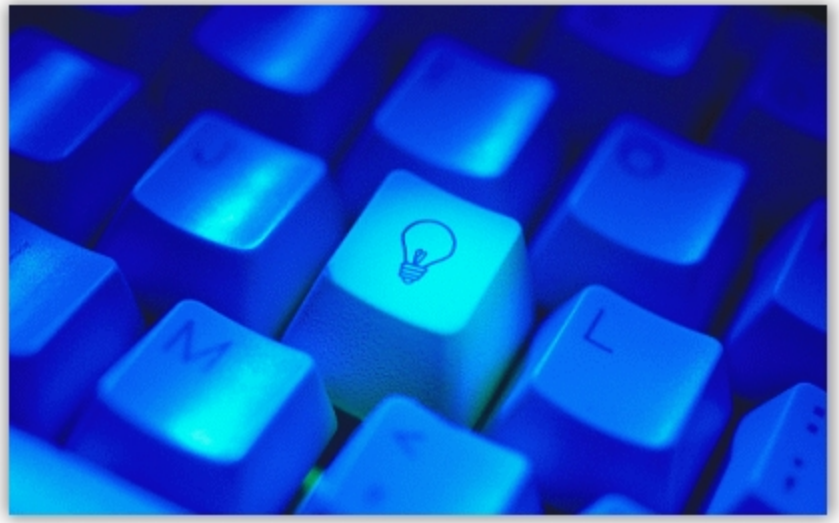


© 2014 ServiceNow All Rights Reserved

Tracing In Fiddler



© 2014 ServiceNow All Rights Reserved



Hands-On Lab #3

Trace your own SAML Logon

© 2014 ServiceNow All Rights Reserved

OpenAM – Demo

https://community.servicenow.com/people/jason.petty/blog/2013/04/05/2638

© 2014 ServiceNow All Rights Reserved

ADFS – Demo

http://wiki.servicenow.com/index.php?title=Configuring_ADFS_2.0_to_Communicate_with_SAML_2.0

© 2014 ServiceNow All Rights Reserved

SAML 2.0: On-Demand Login/User Provisioning

https://community.servicenow.com/message/683704

© 2014 ServiceNow All Rights Reserved

Top Takeaways

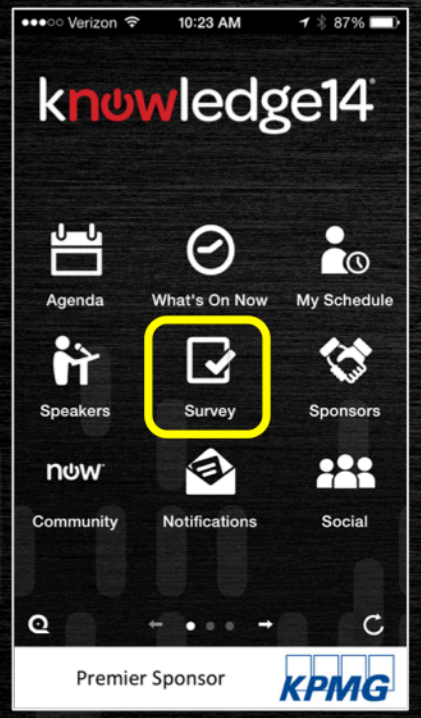
1 Know how SAML 2.0 works

2 Know how to setup and configure SAML 2.0 in a ServiceNow instance

3 Know what tools you can use to troubleshoot

© 2014 ServiceNow All Rights Reserved

Tell us what you think!



Click on the survey link in your Knowledge14 mobile app. Help us make Knowledge 15 even more valuable!

Thank You

Jason Petty

Expert Services

ServiceNow

jason.petty@servicenow.com

Jonatan Jardi

Senior Technical Consultant

ServiceNow

jonatan.jardi@servicenow.com

Want a copy of this deck?

Sign into the BuzzHub to unlock all the slides and lab guides from Knowledge14 sessions

