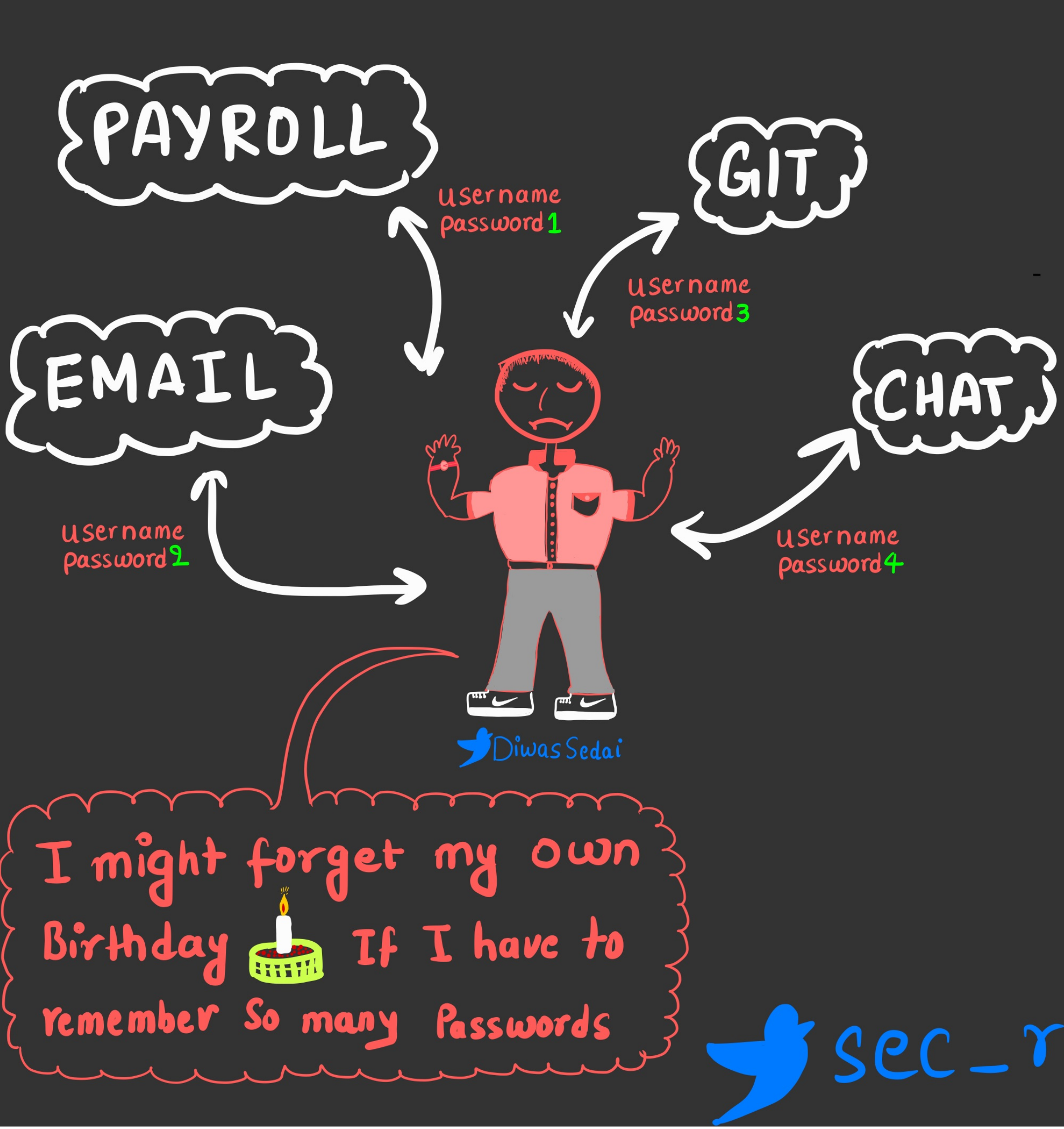
SECURITY ASSERTION MARKUP LANGUAGE

"SAML"



sec_r0

I am Rohit !!!

sec_r0

As a Developer try easing out user experience with SAML .....

Are you aware of SAML ?

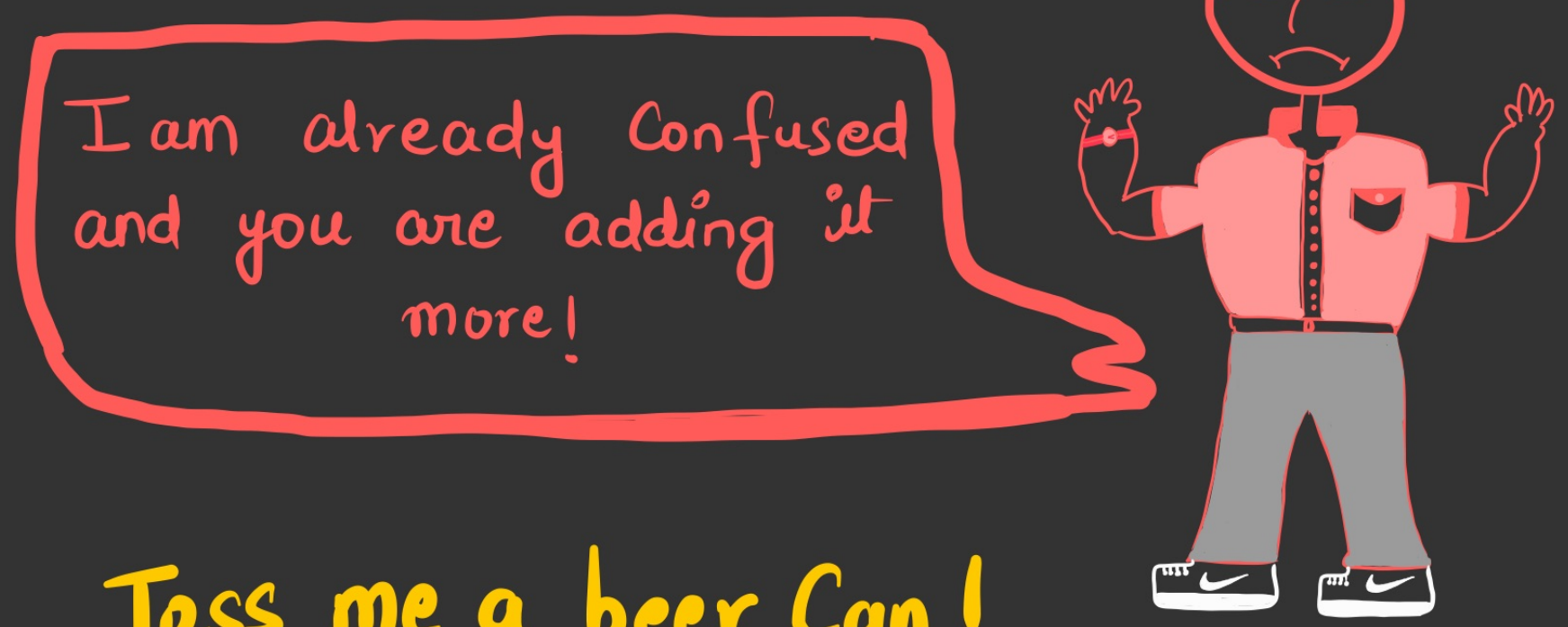
SAML ??

Nice name for a CowGirl what does that mean ?

HA HA !!

Not a CowGirl , but a technique so that all users have to remember only one password and login only in one portal .....

SAML is an open standard that Allows Identity Providers (Idp) to pass authurization credentials to service providers.



Toss me a beer Can!
& my nerve will open.

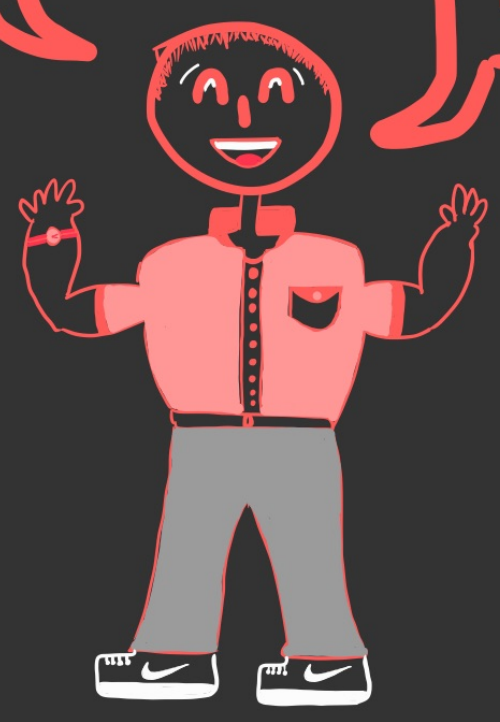
High level flow.

SAML can help you use one set of credentials To log into various websites

sec_r0

So I can use one set of Credentials to access all my web applications...

That's miracle



<XML>
{ Authentication & Authorization } Data
</XML>

SAML Response

SAML is an XML standard that allows the exchange of authentication and authorization data to be shared between security domain

SAML pack the authN & authZ data in SAML assertion

Called SAML Token also.

sec_r0

* SAML works by passing users, logins and attribute between Idp & Service provider

So for user overall task is to authenticate to Idp and later Service provider Grants you access.

There are 3 Actors Involved

USER

That's You

Identity Provider [Idp]

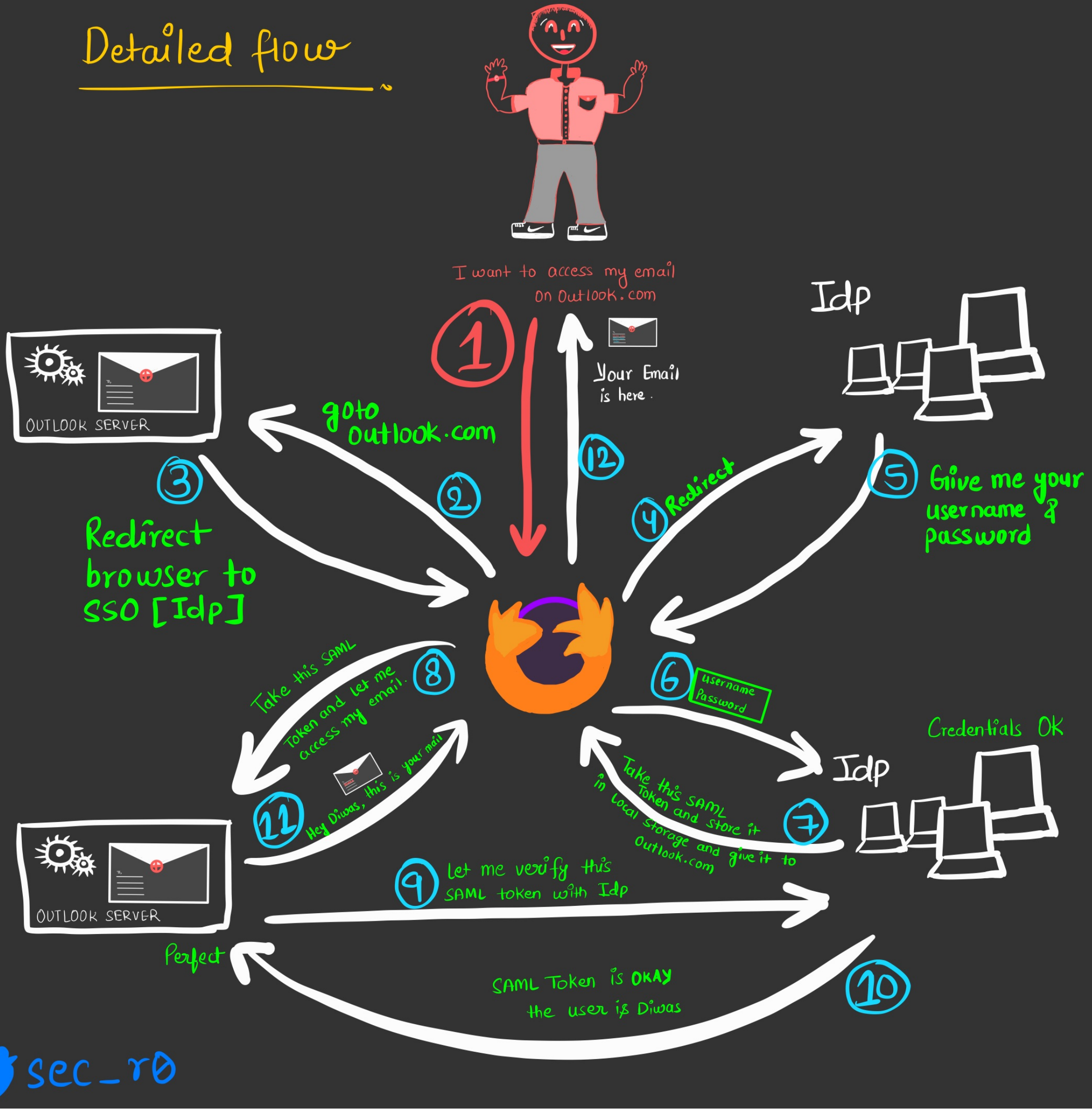
You will have account here and it will authenticate you to Service.

Service provider [SP]

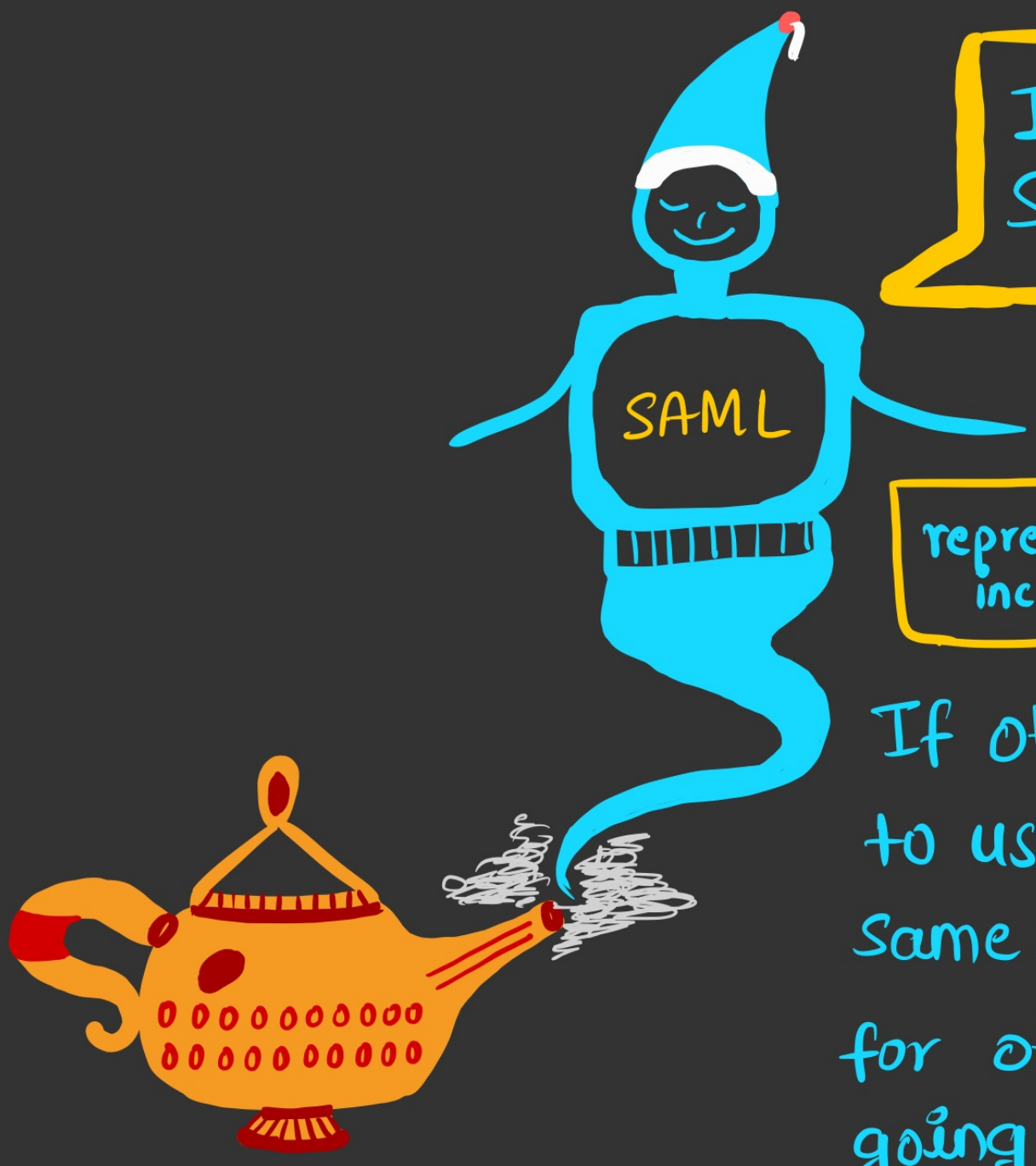
The Stuff you want to access

* Suppose your organization uses Outlook as Email platform. Whenever you try to access Outlook, It will redirect you to Organization's SSO (Single Sign On) Service. The SSO will authenticate you and reply a SAML Response [SAML ASERTION]

Detailed flow



sec_r0



I did the magic from Step 3 to 10

Step 9-10 are just logical representation, the verification may be included inside SAML token

If other services also configures to use the same Idp then same Saml token can be used for other services without going to 3-8

* Step 9 & 10 is offline Validation.
  ↳ i.e token verification

* Idp signs the SAML response through X.509 Certificate

* Service provider Since It already knows Idp, Knowns the X.509 Certificate finger print.

* So Service provider validates SAML response By validating the Response with the Signature

SAML is a bulky Response document & it may look something like this. Lets Notice few important field

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="_8e8dc5f69a98cc4c1ff3427e5ce34606fd672f91e6"
Version="2.0" IssueInstant="2014-07-17T01:01:48Z" Destination="http://sp.example.com/demo1/index.php?
acs" InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685">
  <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/
2001/XMLSchema" ID="pfx396068f0-603c-34b5-2ffd-ce741a420fba" Version="2.0"
IssueInstant="2014-07-17T01:01:48Z">
    <saml:Issuer>http://idp.example.com/metadata.php</saml: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/2000/09/xmldsig#rsa-sha1"/>
  <ds:Reference URI="#pfx396068f0-603c-34b5-2ffd-ce741a420fba"><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/
2000/09/xmldsig#sha1"/><ds:DigestValue>CKOBg5WsVUfNekG8JrwUwTvvRtM=</ds:DigestValue></ds:Reference></
ds:SignedInfo><ds:SignatureValue>MgSNyQZ7q8MzgX2ho3YPCMITqxw6wi5DhK0Qn0cR43AqtLmxFs9CiwZxPUf03nh1WBg2f70
Qf3EG4WxmzfgWmvJLUFczZ2sfyZJuYw2j97odBsmi+kLumM9w9mroJjoUhFW0+0Ivo8NY8pFDjiQZ8zLrQwI+VOOIhbs0g9K44lA </
ds:SignatureValue>
<ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIICajCCAdOgAwIBAgIBADANBgkqhkiG9w0BAQ0FADBSMQswCQYDVQQGEwJ
1czETMBEGA1UECAwKQ2FsaWZvcm5pYTEVMBMGA1UECgwMT25lbG9naW4gSW5jMRcwFQYDVQQDDA5zcC5leGFtcGxlLmNvbTAeFw0xNDA
3MTcxNDEyNTZaFw0xNTA3MTcxNDEyNTZaMFIxCzAJBgNVBAYTAnVzMRMwEQYDVQQIDApDYWxpZm9ybmlhMRUwEwYDVQQKDAxPbmVsb2d
pbiBJbmMxFzAVBgNVBAMMDnNwLmV4YW1wbGUuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDZx+ON4IUoIWxgukTb1tOiX3b
MYzYQiwWPUNMp+Fq82xoNogso2bykZG0yiJm5o8zv/sd6pGouayMgkx/
2FSOdc36T0jGbCHuRSbtia0PEzNIRtmViMrt3AeoWBidRXmZsxCNLwgIV6dn2WpuE5Az0bHgpZnQxTKFek0BMKU/
d8wIDAQABo1AwTjAdBgNVHQ4EFgQUGHxYqZYyX7cTxKVODVgZwSTdCnwwHwYDVR0jBBgwFoAUGHxYqZYyX7cTxKVODVgZwSTdCnwwDAY
DVR0TBAUwAwEB/zANBgkqhkiG9w0BAQ0FAAOBgQByFOl+hMFICbd3DJfnp2Rgd/dqttsZG/tyhILWvErbio/
DEe98mXpowhTkC04ENprOyXi7ZbUqiicF89uAGyt1oqgTUCD1VsLahqIcmrzgumNyTwLGWo17WDAa1/usDhetWAMhgzF/
Cnf5ek0nK00m0YZGyc4LzgD0CROMASTWNg==</ds:X509Certificate></ds:X509Data></ds:KeyInfo></ds:Signature>
    <saml:Subject>
      <saml:NameID SPNameQualifier="http://sp.example.com/demo1/metadata.php"
Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:transient">_ce3d2948b4cf20146dee0a0b3dd6f69b6cf86f62d7</saml:NameID>
      <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData NotOnOrAfter="2024-01-18T06:21:48Z" Recipient="http://
sp.example.com/demo1/index.php?acs" InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685"/>
      </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2014-07-17T01:01:18Z" NotOnOrAfter="2024-01-18T06:21:48Z">
      <saml:AudienceRestriction>
        <saml:Audience>http://sp.example.com/demo1/metadata.php</saml:Audience>
      </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2014-07-17T01:01:48Z" SessionNotOnOrAfter="2024-07-17T09:01:48Z"
SessionIndex="_be9967abd904ddcae3c0eb4189adbe3f71e327cf93">
      <saml:AuthnContext>
        <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</
saml:AuthnContextClassRef>
      </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
      <saml:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">test</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="mail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">test@example.com</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="eduPersonAffiliation" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
        <saml:AttributeValue xsi:type="xs:string">users</saml:AttributeValue>
        <saml:AttributeValue xsi:type="xs:string">examplerole1</saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
  </saml:Assertion>
</samlp:Response>
```

↳ After Idp Authenticates, user will be routed to this URI with SAML Token

↳ Signature - Digest

↳ This Response is targetted for this service

List of SAML attributes belonging to authenticated user

value of uid

This SAML response contains uid, mail etc fields in Response document

of mail attribute

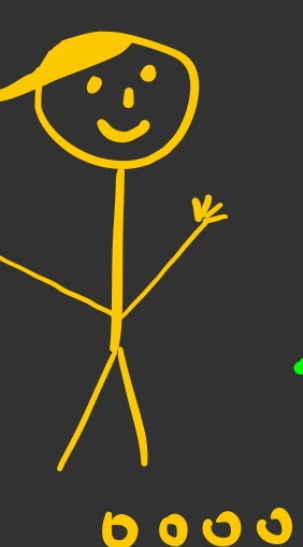
string

value

Multi valued field example

sec_r0

* Ignore other fields



- Next time for some other Service provider which is configured with Same Idp, User need not to authN again.

- Idp knows user has already logged in, so it will just Create another SAML response.

- And the flow is same.

Enhanced UX.

So I need to remember Only single Credentials.

And You saved my day to learn SAML

Here is another  CHEERS!

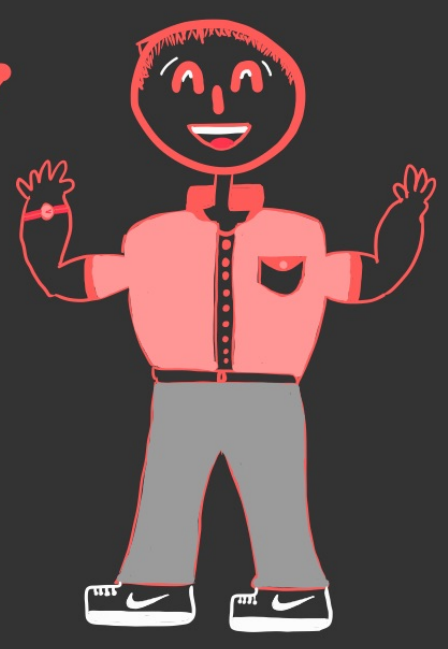
I hope You Enjoyed this !

thanks for reading

Join for updates

Read more Zines
@
securityzines.com

A big thanks to Diwas for helping with Content



Diwas Sedai