Multifactor Authentication Challenges

Jeremy Duncan

Tachyon Dynamics

jduncan@tachyondynamics.com

Information Security Principle

- **Non-Repudiation**: “one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction”
- Without this, authentication fails or breaks

MFA and Implementation Challenges

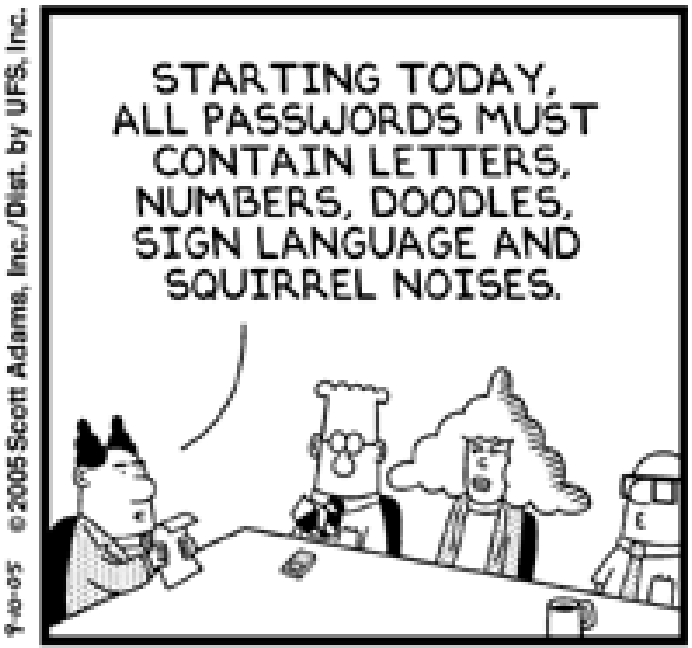
- What is MFA
- What is **not** MFA
- How can you implement MFA for your organization
- What are some good operational examples

MFA is…

- Single Sign-On
- More than one factor
  - Something you have
  - Something you know
  - Something you are
- Again, single sign-on
  - Must chain the mechanisms into one user

Something you know

- A username and password
- A PIN to unlock a hardware or software token



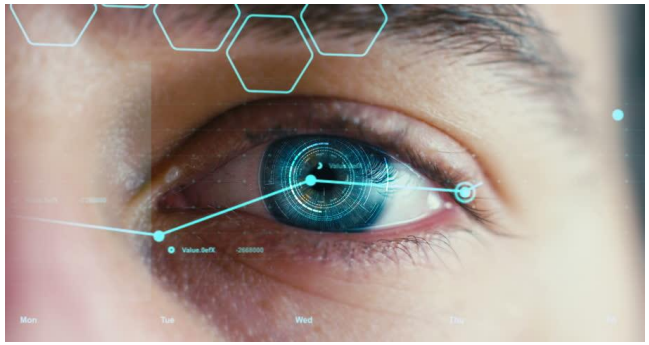
Something you have

- A disconnected token – Time Based (RSA SecurID with numeric screen output)
- A connected token (a USB-connected Yubikey One-Time Password (OTP) generator
- A smartcard, a USB connected hardware token

Tachyon Dynamics

Something you are

- Biometrics
- Finger prints, Retina scans, Face ID, etc



Single Sign On

- All factors **MUST CHAIN TOGETHER**
- Otherwise you can't secure non-repudiation!
- Examples:
  - DoD PKI authentication: smart card login, mapped to an authorization database (e.g. Microsoft Active Directory)
  - Active Directory with OTP token: username and password in active directory with a one-time-use token like Yubikey

Send it to SAML!

- SAML allows for a SSO service to handle for everyone else
  - Think login with Google or Facebook
- For web UI's works well
- For client applications doesn't work so well (Java applications, CLI/SSH logins, etc)
- Examples are:
  - ADFS, Centrify, DoD IdAM, iSAML, SimpleSAML, etc

What is **not** MFA

- 2-step verification (i.e. passcode sent via SMS to your phone)
  - Still the same factor (something you know) as it can be obtained from the network
- Client SSL certificate, and then a separate username and password
  - Violates non-repudiation – not chained together
- Just biometrics

Are Biometrics secure?

- Using biometrics
  - Controversial topic
- What happens when your fingerprint / face / retina is compromised? You can't grow a new one, but you can change a password…

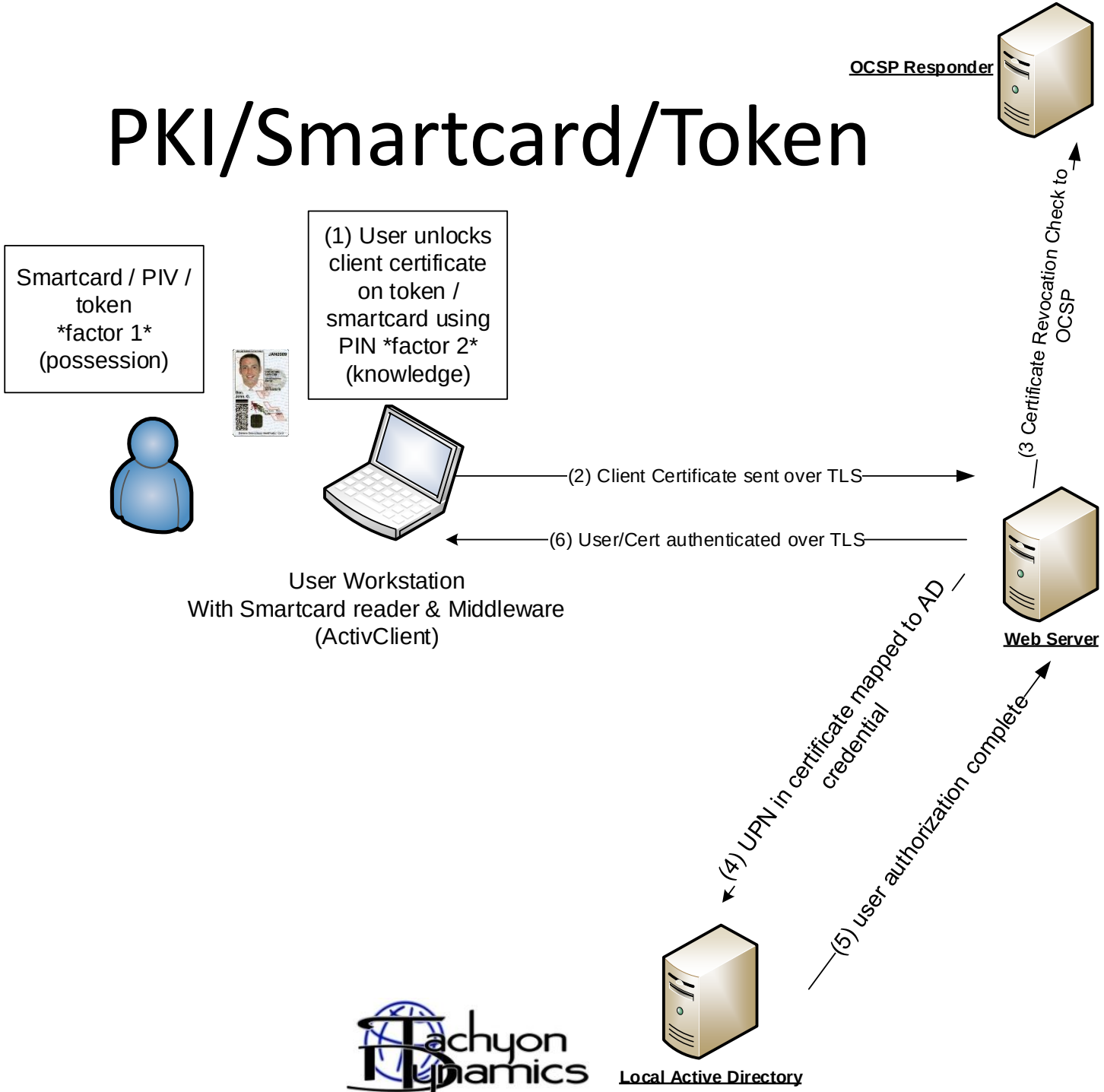
How to implement MFA

- Pick at least 2 factors (know, have, are)
  - Recommend staying away from biometrics for now
- Integrate a single sign-on into all mechanisms
  - Map smartcard UPNs to Active Directory
  - Use SAML IDP for things that can't do certificate authentication
- Implement different forms
  - Yubikey and RADIUS/AD for CLI/SSH
- PIV for smartcard-like

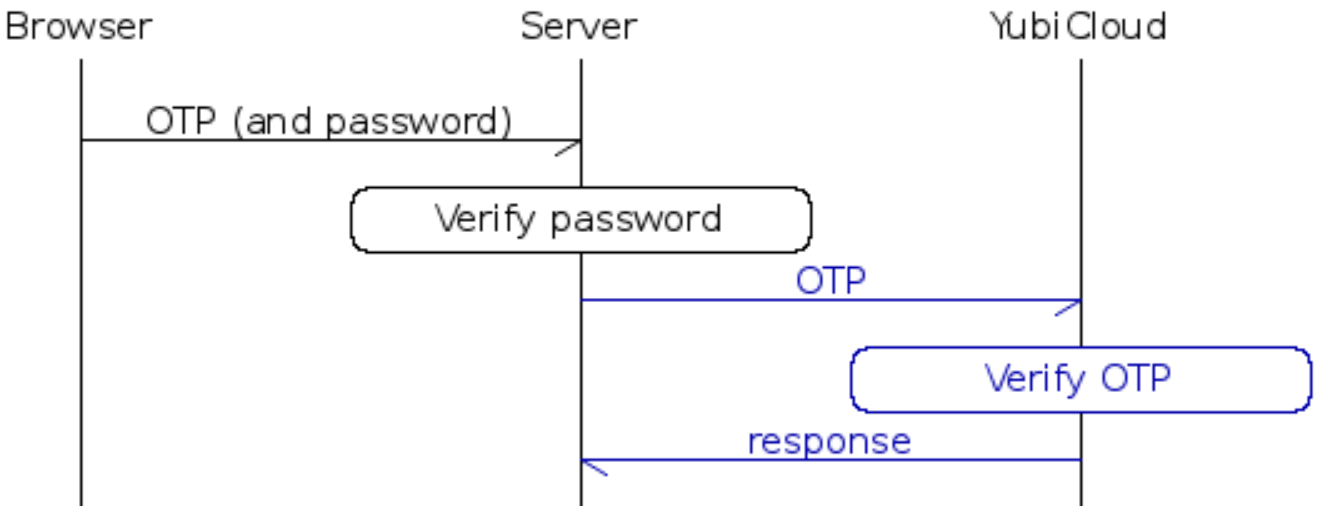
Operational Examples of MFA

- DoD PKI / Common Access Card / Smartcard
- Hardware Token One Time Passcode (HOTP)
- SAML

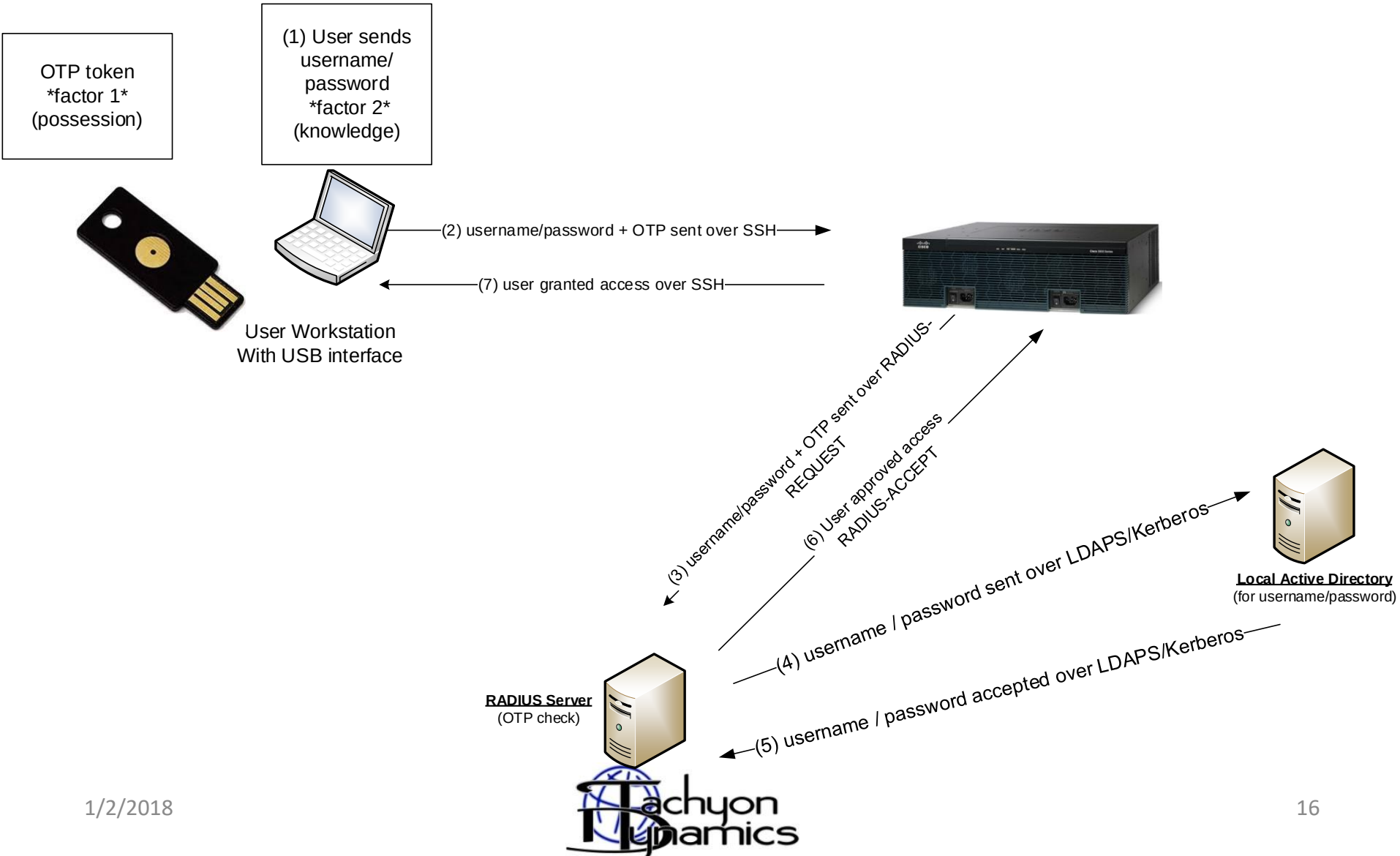
PKI/Smartcard/Token



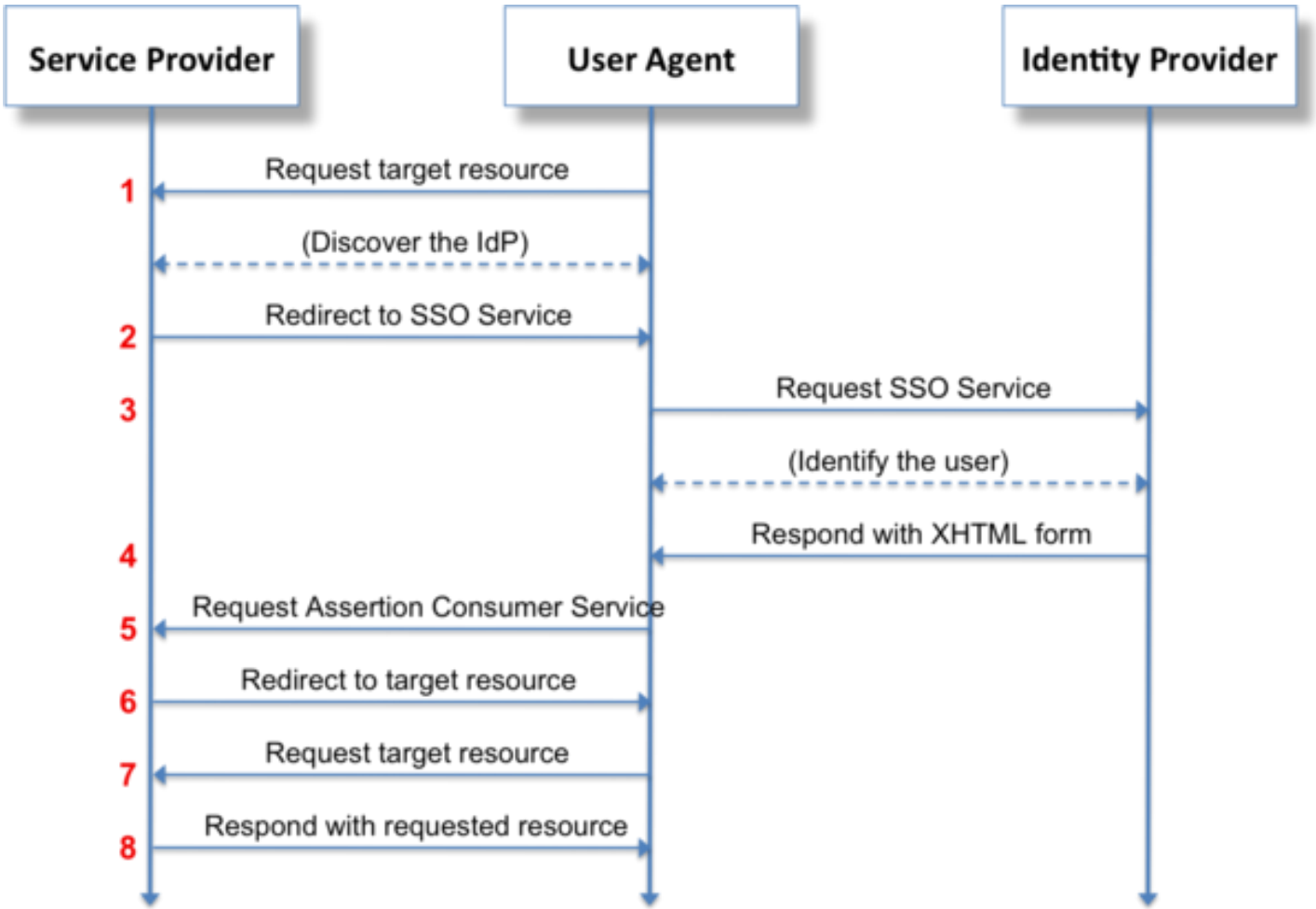
OTP (Yubicloud)



OTP (Yubikey/AD)



SAML SSO / IDP


Service Provider
User Agent
Identity Provider
1
Request target resource
(Discover the IdP)
2
Redirect to SSO Service
3
Request SSO Service
(Identify the user)
4
Respond with XHTML form
5
Request Assertion Consumer Service
6
Redirect to target resource
7
Request target resource
8
Respond with requested resource

Questions?

Jeremy Duncan

Tachyon Dynamics

@TachyonDynamics

@nacnud

jduncan@tachyondynamics.com

https://www.tachyondynamics.com