

T&I Incubator: OIDC Support for SSH Client

Sprint demo #4.3 – 1st June 2021

Dmytro Dehtyarov

Public

www.geant.org



Agenda

- Background & Motivation
- Requirements
- High-level architecture
- Activities
- Next steps



Motivation

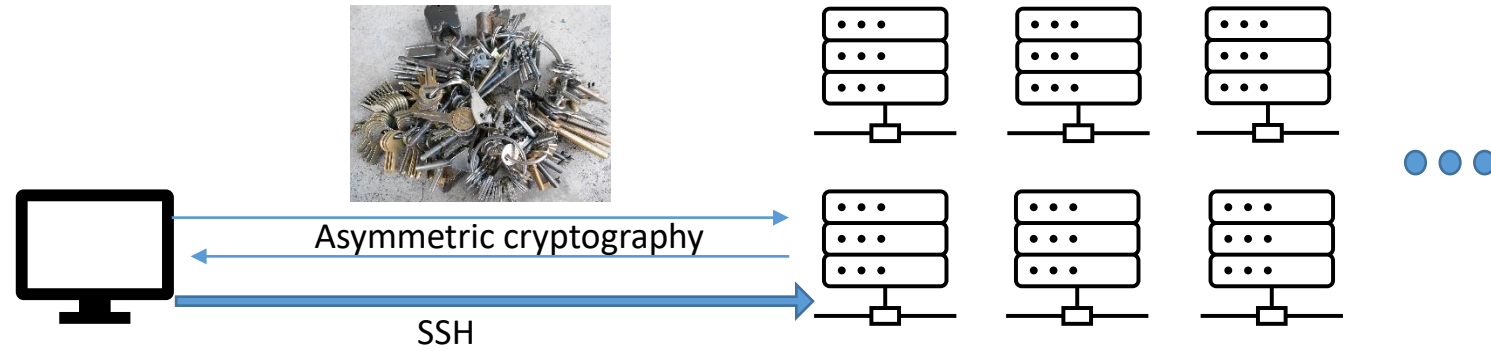
- SSH Key Management
 - Risks of untracked and unmanaged SSH Keys
 - 90% of keys are no longer used [1]
 - Scalability issues
-
- ... “SSH key management can get so complicated that you’ll be best advised to stop using SSH keys” [3]



[2]

Motivation

- Scalability issues:

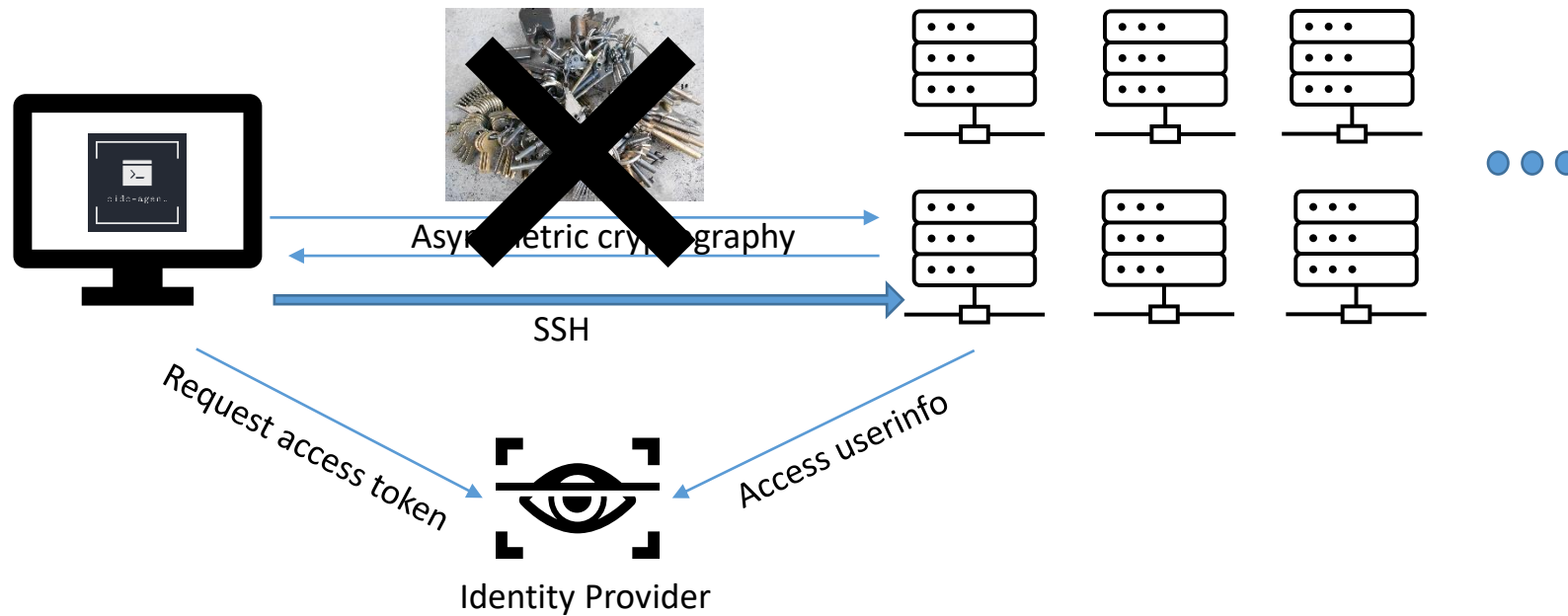


- Improvements:
 - Policies
 - Rotation
 - Remediation

Motivation

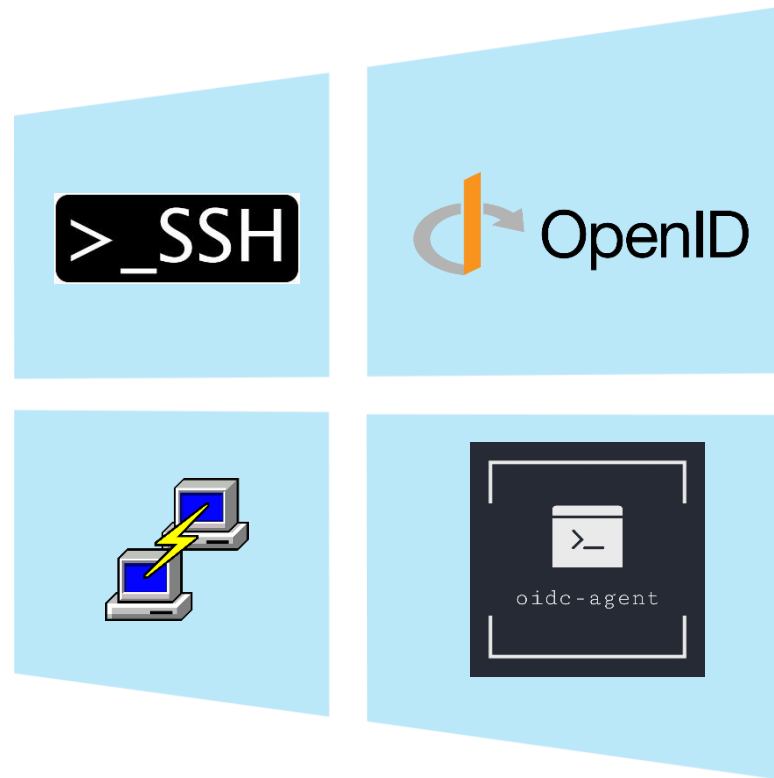


Access Tokens!



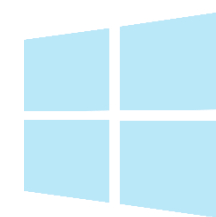
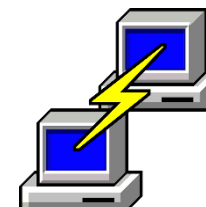
Goals

- High-Level: Integrate OIDC with SSH (client-side) under **Windows**
- Port oidc-agent to Windows
- Integrate oidc-agent into SSH client Putty



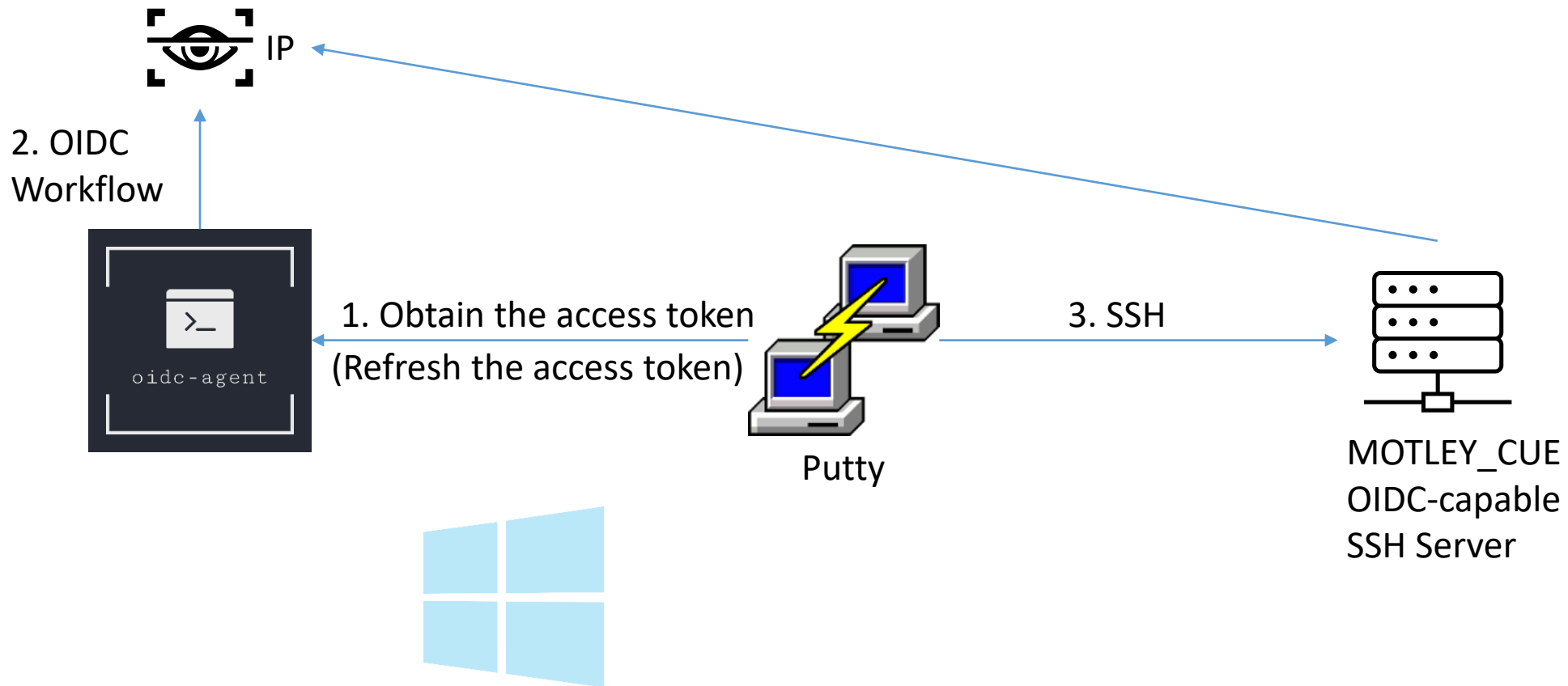
Requirements

- oidc-agent obtains/manages access tokens on Windows
- oidc-agent must be easy-to-install on Windows
- oidc-agent runs as a daemon (Windows Service) providing an API
- putty allows to select between ssh-keys and oidc-tokens (pageant VS. oidc-agent)
- putty supports authentication&authorization with oidc-tokens against supported ssh-server
- putty obtains valid access tokens from oidc-agent
- putty provides a simple GUI for oidc-gen

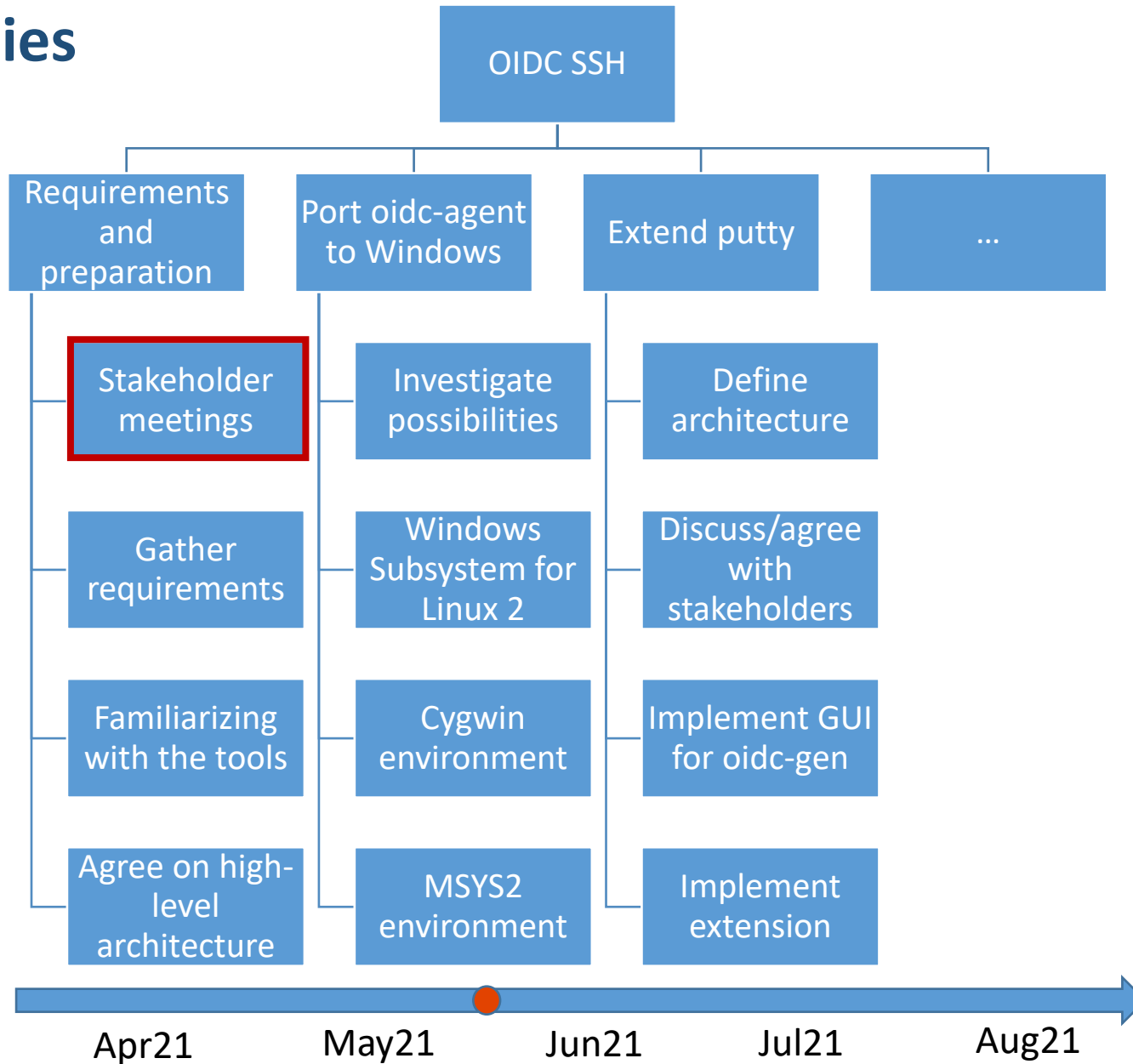


High-Level Architecture

- oidc-agent replaces pageant (ssh-agent)

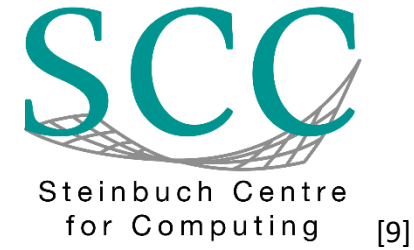


Activities

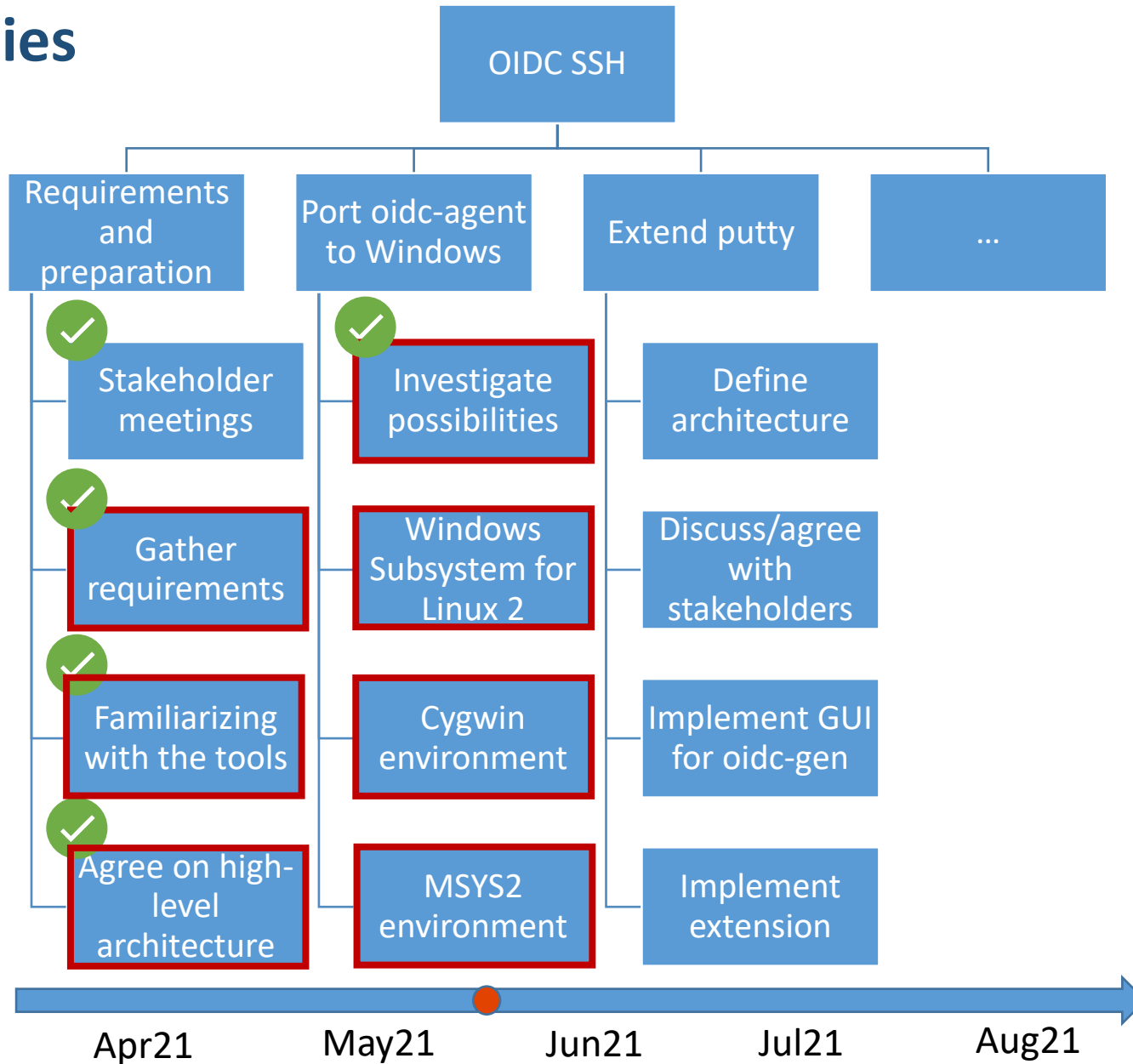


Stakeholders

- oidc-agent developer @SCC
- oidc-ssh developer @SCC
- putty developer
- Nikhef
- T&I Incubator



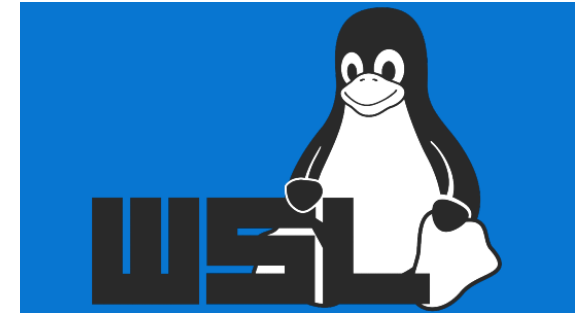
Activities



Possibilities to port oidc-agent

1. Windows Subsystem for Linux 2

- GNU/Linux environment
- Less overhead than Dual Boot/VM
- Not user-friendly (esp. WinEducation)



[11]

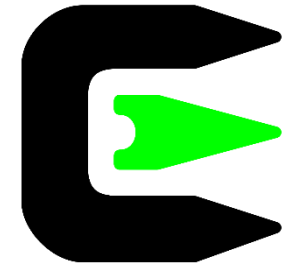
```
dimonua@finrod2: ~  
dimonua@finrod2:~$ eval `oidc-keychain`  
oidc-keychain: Reusing agent pid 29  
dimonua@finrod2:~$ oidc-gen google  
[1] https://accounts.google.com/  
[2] https://iam-test.indigo-datacloud.eu/  
[3] https://iam.deep-hybrid-datacloud.eu/  
[4] https://iam.extreme-datacloud.eu/  
[5] https://iam-demo.cloud.cnaf.infn.it/  
[6] https://b2access.eudat.eu/oauth2/  
[7] https://b2access-integration.fz-juelich.de/oauth2  
[8] https://unity.eudat-aai.fz-juelich.de/oauth2/  
[9] https://login-dev.helmholtz.de/oauth2/  
[10] https://login.helmholtz.de/oauth2/  
[11] https://services.humanbrainproject.eu/oidc/  
[12] https://aai.egi.eu/oidc/  
[13] https://aai-demo.egi.eu/oidc/  
[14] https://aai-dev.egi.eu/oidc  
[15] https://login.elixir-czech.org/oidc/  
[16] https://oidc.scc.kit.edu/auth/realms/kit/  
[17] https://wlcg.cloud.cnaf.infn.it/  
Issuer [https://accounts.google.com/]:
```

Plan B!

Possibilities to port oidc-agent

2. Cygwin Environment

- Large collection of GNU tools
- POSIX API for Windows
- Goals:
 - ✓ • Compile and link oidc-agent sources
 - Exclude unnecessary functionalities
 - Adapt source code for cygwin environment
 - Adapt building procedures
 - 🔄 • Run oidc-agent as a stand-alone application
 - Distribution/Packaging ?
 - cygwin1.dll dependency




[12]

Plan A.1!

Possibilities to port oidc-agent

3. MSYS2

- Tools and libraries for building native WinApps
- Native = against Windows APIs
- No external dependencies / (ideally) No POSIX emulation layer
- Goals:
 -  Compile and link oidc-agent sources

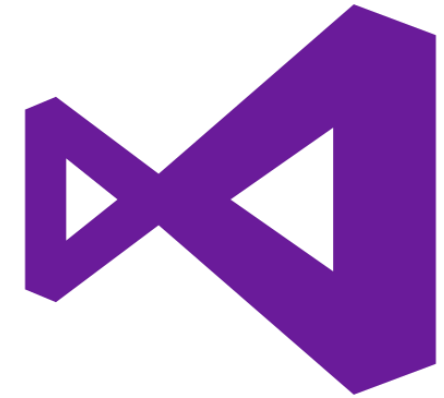


Plan A.2!

Possibilities to port oidc-agent

4. Build natively in VisualStudio

- Goal: rewrite platform-dependent code for Windows
- Major dependencies are available for Windows too



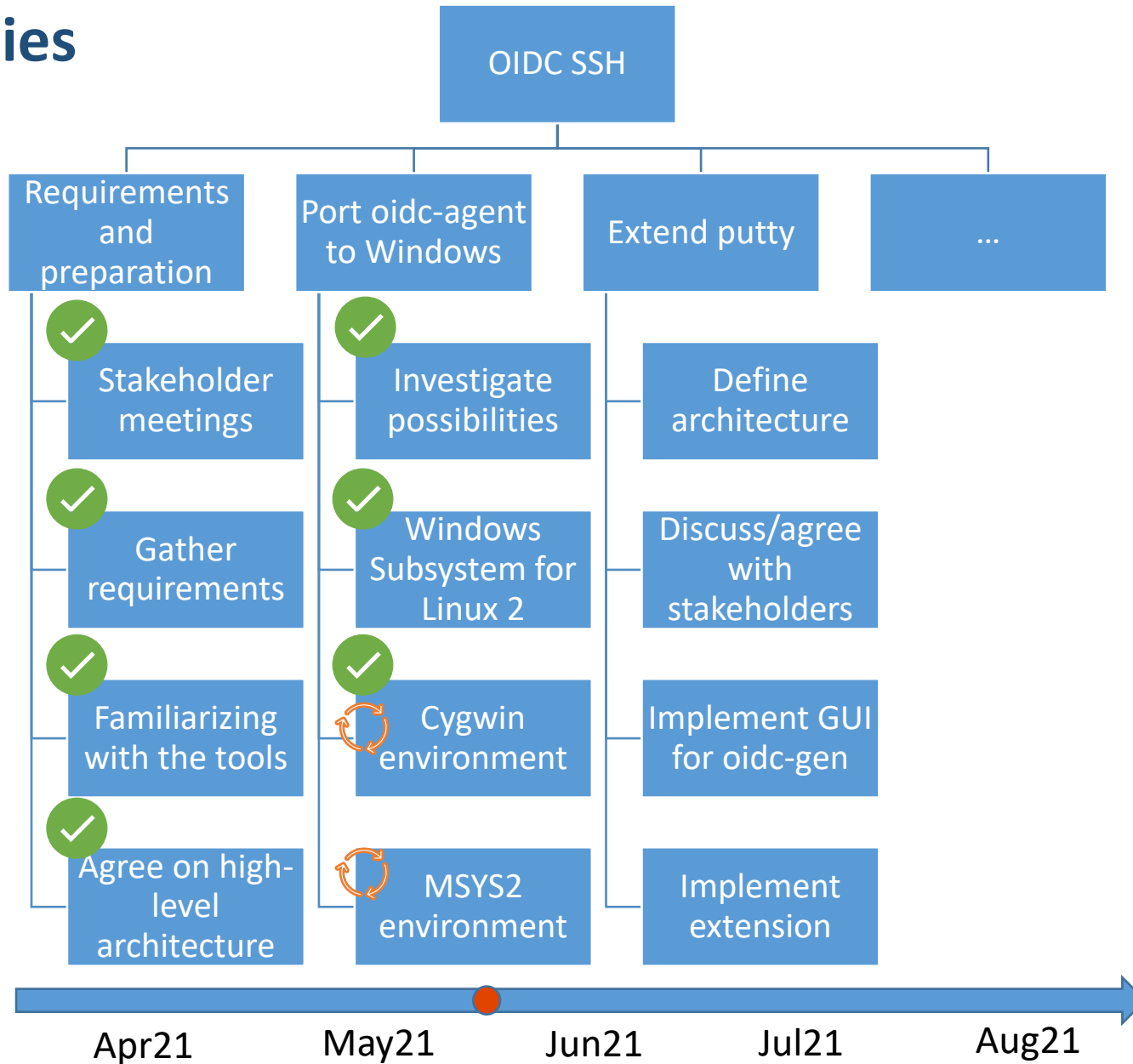
[14]



Libmicrohttpd [16]

Plan C!

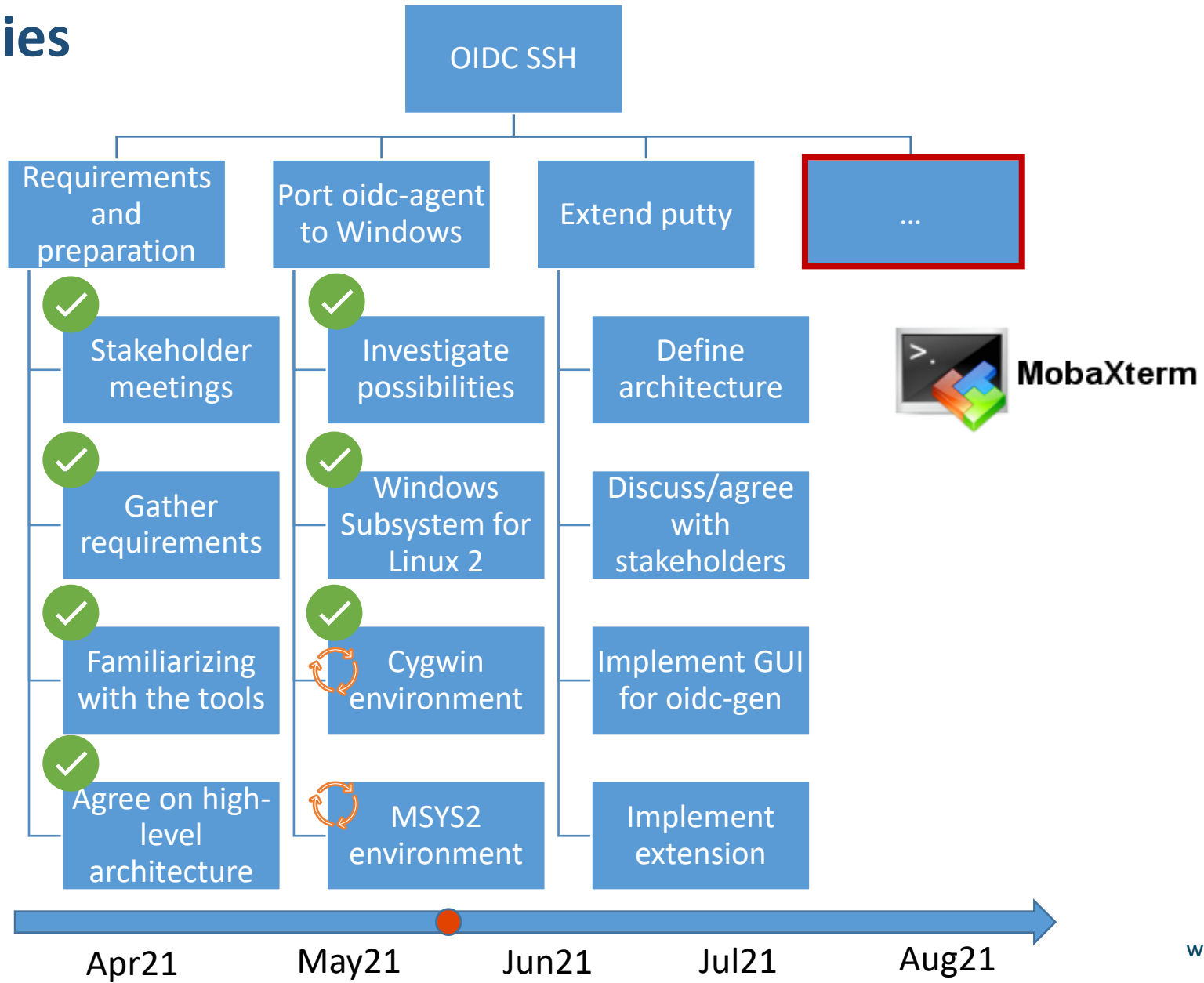
Activities



Next steps

- Package oidc-agent as a stand-alone app (Cygwin/Msys2)
- Investigate and agree on architecture for putty extension
- Implement GUI for oidc-gen
 - Generate account configurations
- Implement putty extension for OIDC tokens

Activities



Thank you

Any questions?

www.geant.org



References

- [1] <https://www.ssh.com/academy/iam/ssh-key-management>
- [2] <https://images.app.goo.gl/8CTV52CRGRxJrBRLA>
- [3] <https://goteleport.com/blog/ssh-key-management/>
- [4] <https://images.app.goo.gl/jzgLw2zjqKzwi7cp9>
- [5] <https://images.app.goo.gl/tKo77xxstdu1DUJr5>
- [6] <https://images.app.goo.gl/bUgQzq5YaTPamEXP8>
- [7] <https://github.com/indigo-dc/oidc-agent/blob/master/logo.png>
- [8] <https://images.app.goo.gl/TJy4y5WigecQJ3sU7>
- [9] <https://images.app.goo.gl/rBFwLMwiterHN9Av5>
- [10] <https://images.app.goo.gl/K4QzEyU7Q2P2sqoj8>
- [11] <https://docs.microsoft.com/en-us/windows/wsl/>
- [12] <https://images.app.goo.gl/CBiCK5SqUDRksqt69>
- [13] <https://images.app.goo.gl/M1eHHZSzY1cc9X37A>
- [14] <https://images.app.goo.gl/Jaxk9RcesMzGCcS99>
- [15] <https://images.app.goo.gl/jzXenF4tMquP19HCA>
- [16] <https://images.app.goo.gl/KTBckfa6R4mibR8z9>