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]
Motivation

• Scalability issues:

• Improvements:
  • Policies
  • Rotation
  • Remediation
Motivation

Access Tokens!

Asymmetric cryptography

SSH

Identity Provider

Request access token

Access userinfo
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)

1. Obtain the access token (Refresh the access token)
2. OIDC Workflow
3. SSH

MOTLEY_CUE
OIDC-capable
SSH Server

IP
Activities

OIDC SSH

Requirements and preparation
- Stakeholder meetings
- Gather requirements
- Familiarizing with the tools
- Agree on high-level architecture

Port oidc-agent to Windows
- Investigate possibilities
- Windows Subsystem for Linux 2
- Cygwin environment
- MSYS2 environment

Extend putty
- Define architecture
- Discuss/agree with stakeholders
- Implement GUI for oidc-gen
- Implement extension

Apr21 May21 Jun21 Jul21 Aug21
Stakeholders

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

OIDC SSH

Requirements and preparation
- Stakeholder meetings
- Gather requirements
- Familiarizing with the tools
- Agree on high-level architecture

Port oidc-agent to Windows
- Investigate possibilities
- Windows Subsystem for Linux 2
- Cygwin environment
- MSYS2 environment

Extend putty
- Define architecture
- Discuss/agree with stakeholders
- Implement GUI for oidc-gen
- Implement extension

Apr21 May21 Jun21 Jul21 Aug21
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)

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
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

Plan C!
Activities

OIDC SSH

Requirements and preparation
- Stakeholder meetings
- Gather requirements
- Familiarizing with the tools
- Agree on high-level architecture

Port oidc-agent to Windows
- Investigate possibilities
- Windows Subsystem for Linux 2
- Cygwin environment
- MSYS2 environment

Extend putty
- Define architecture
- Discuss/agree with stakeholders
- Implement GUI for oidc-gen
- Implement extension

...
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

OIDC SSH

Requirements and preparation
- Stakeholder meetings
- Gather requirements
- Familiarizing with the tools
- Agree on high-level architecture

Port oidc-agent to Windows
- Investigate possibilities
- Windows Subsystem for Linux 2
- Cygwin environment
- MSYS2 environment

Extend putty
- Define architecture
- Discuss/agree with stakeholders
- Implement GUI for oidc-gen
- Implement extension

Apr21 May21 Jun21 Jul21 Aug21
Thank you

Any questions?

www.geant.org
References

[1] https://www.ssh.com/academy/iam/ssh-key-management
[3] https://goteleport.com/blog/ssh-key-management/
[6] https://images.app.goo.gl/bUgQzq5YaTPamEXP8
[8] https://images.app.goo.gl/TJy4y5WigecQJ3sU7
[10] https://images.app.goo.gl/K4QzEyU7Q2P2sqoj8
[13] https://images.app.goo.gl/M1eHHZSzY1cc9X37A