

Red Hat  
**Summit**

**Connect**

# You Shall Not Pass!

Schutz von Ansible-Inhalten





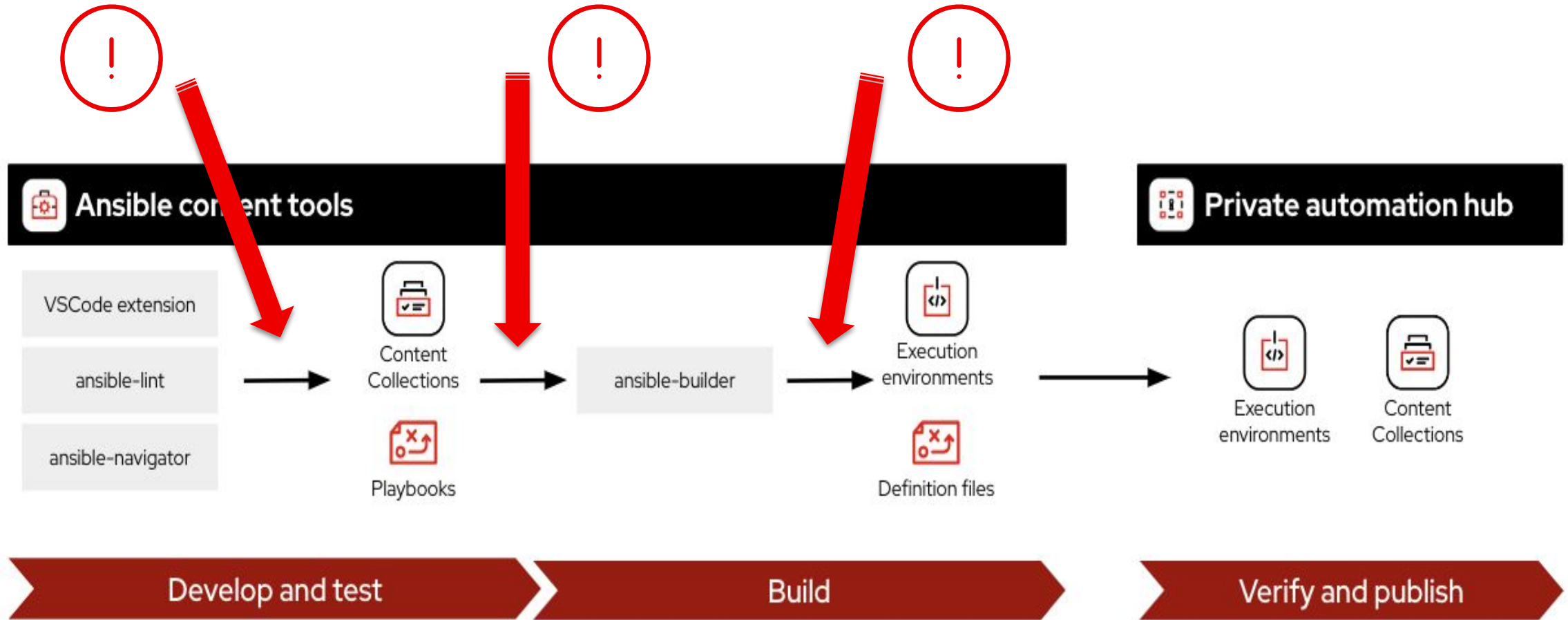
# Dr. Jason Breitweg

Senior Ansible Technical Account Manager  
Red Hat

# What we'll discuss today

- Supply chain attack vectors
- Deeper look into Ansible Content signing
- Ansible Content Collection signing
- Execution Environment signing
- Project signing and verification

# Possible supply chain attack vectors for automation



# A deeper look into Ansible content signing

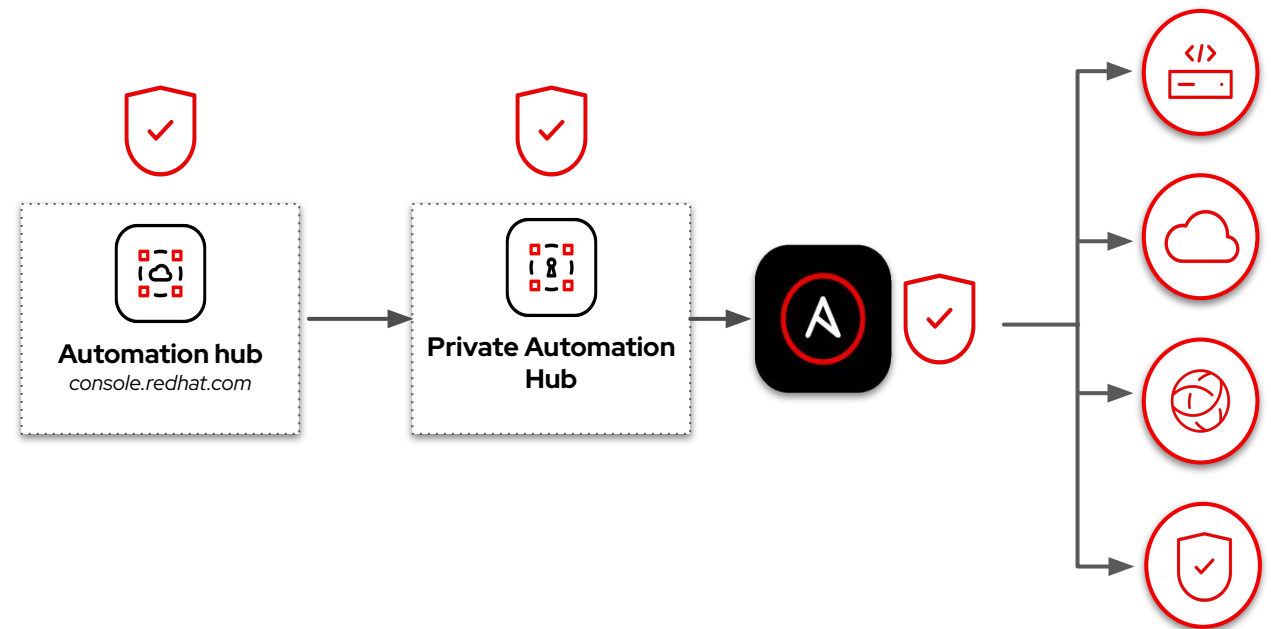
# Chain of custody features

## Automation hub and Red Hat Ansible Certified Content

Red Hat Ansible Certified Content is digitally signed to ensure data integrity and verify content ownership

## Private automation hub

Sign user-built or third-party Ansible Content Collections when publishing to your private automation hub instance



# Signed and certified Ansible Content Collections

[console.redhat.com/ansible/automation-hub](https://console.redhat.com/ansible/automation-hub)

The screenshot displays the 'Collections' page in the Ansible Automation Platform console. The left sidebar contains navigation options: Overview, Automation Hub (with a dropdown), Collections (selected), Partners, Repo Management, Task Management, Connect to Hub, Automation Analytics, Documentation, Red Hat Insights, Inventory, Advisor, Drift, Policies, Register Systems, Remediations, and Tasks. The main content area shows a list of collections with the following details:

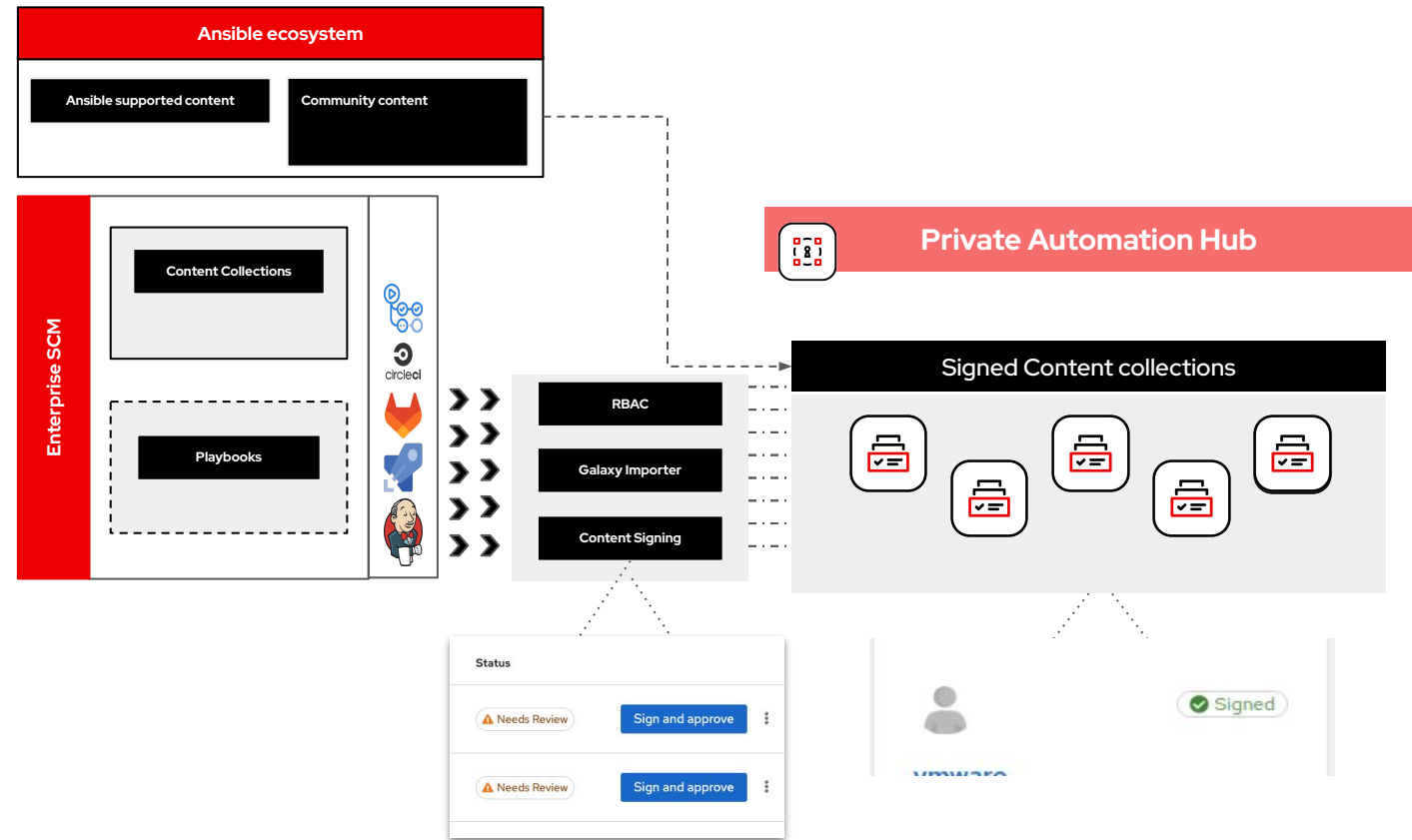
- flasharray**: Provided by Pure Storage. Collection of modules to manage Pure Storage FlashArrays (including Cloud Block Store). 58 Modules, 0 Roles, 0 Plugins, 0 Dependencies. Updated 2 days ago, v1.19.1. Signed.
- scm**: Provided by Ansible. A collection of scm utilities. 2 Modules, 0 Roles, 2 Plugins, 1 Dependency. Updated 3 days ago, v1.0.11. Signed.
- utils**: Provided by Ansible. Ansible Collection with utilities to ease the management, manipulation, and validation of data within a playbook. 4 Modules, 0 Roles, 62 Plugins, 0 Dependencies. Updated 4 days ago, v2.10.3. Signed.
- jws**: Provided by Red Hat, Inc. This collection contains the ansible playbook to setup JWS. 0 Modules, 2 Roles, 0 Plugins, 2 Dependencies. Updated 4 days ago, v1.2.3. Signed.
- ibm\_zos\_cics**: Provided by IBM. The Red Hat Ansible Certified Content for IBM Z CICS collection includes connection plugins, action plugins, modules and sample playbooks to automate tasks for CICS. 5 Modules, 0 Roles, 0 Plugins, 0 Dependencies. Updated 5 days ago, v1.0.5. Signed.

# Ansible Content Collection signing



# Signing Ansible Content Collections

- Private Automation Hub is the library of content for your organization
- It can be enabled to sign collections on upload through a signing service
- Upload Ansible Content Collections to Private Automation Hub using GUI or ansible-galaxy CLI



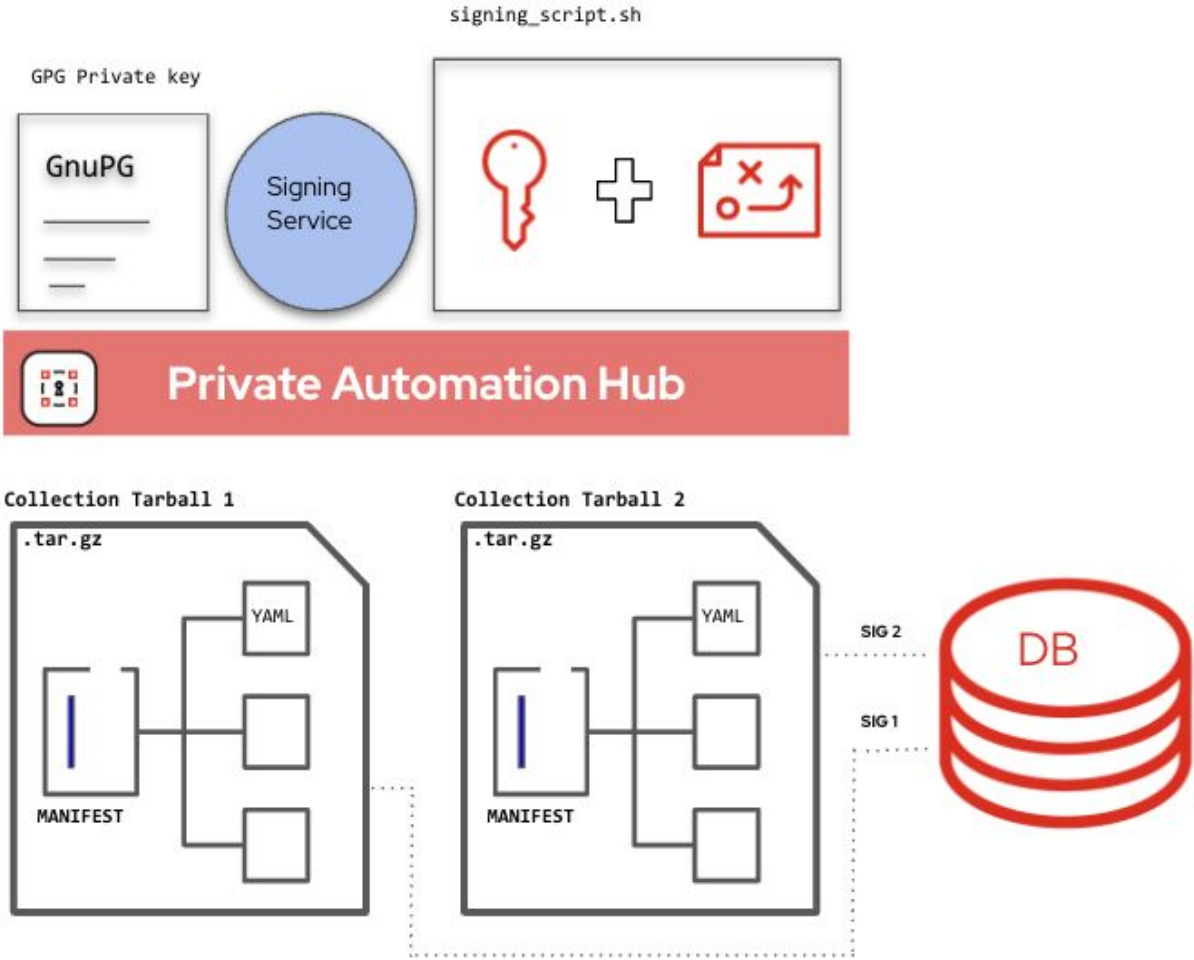
# Install Ansible Automation Hub with signing enabled



- Provide the path to the GnuPG private key
- Provide the path to the signing script
- Enable signing related options

# Collection signing service

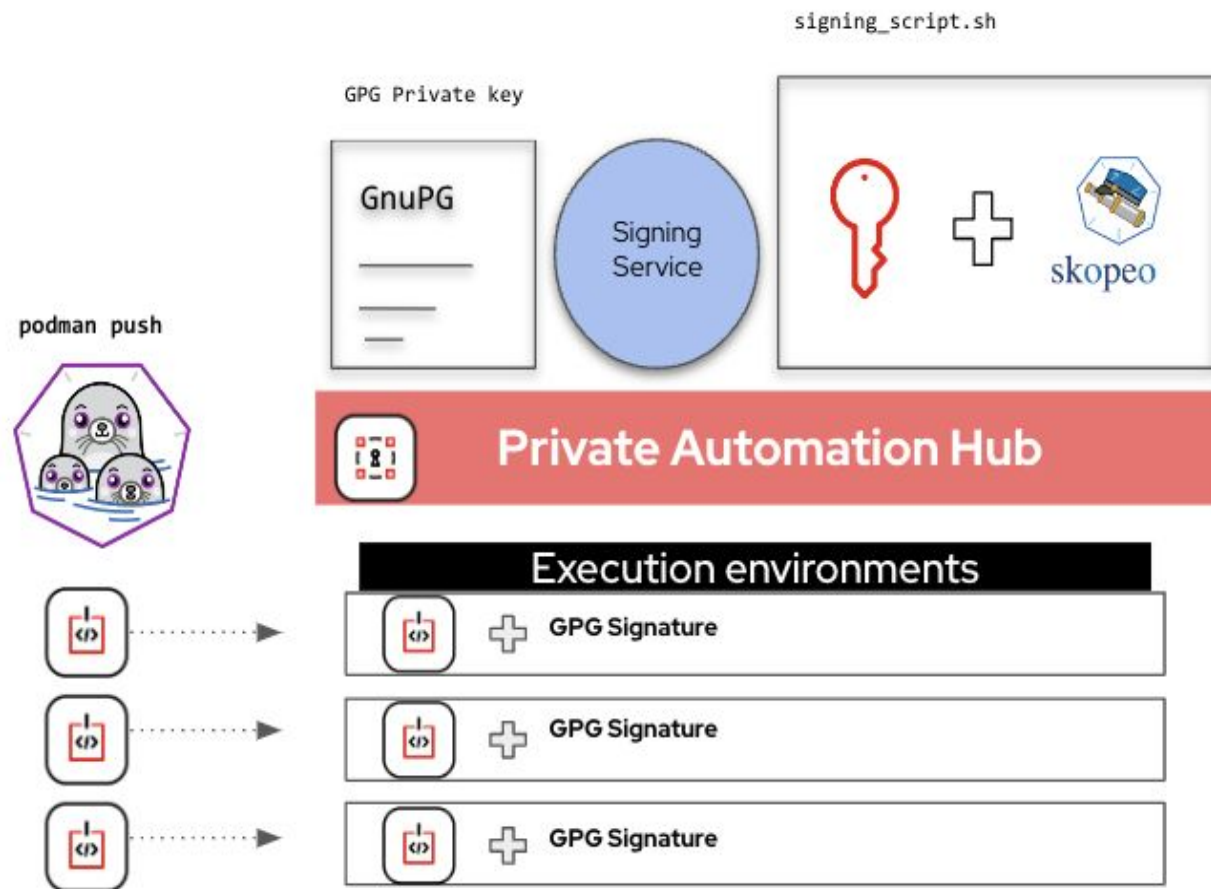
- Signing in Automation Hub is based on GPG
- Signing service holds the GPG key and the signing script
- Signing service performs signing on collection manifest and stores the signatures in the Automation Hub database for each collection



# Execution Environment signing

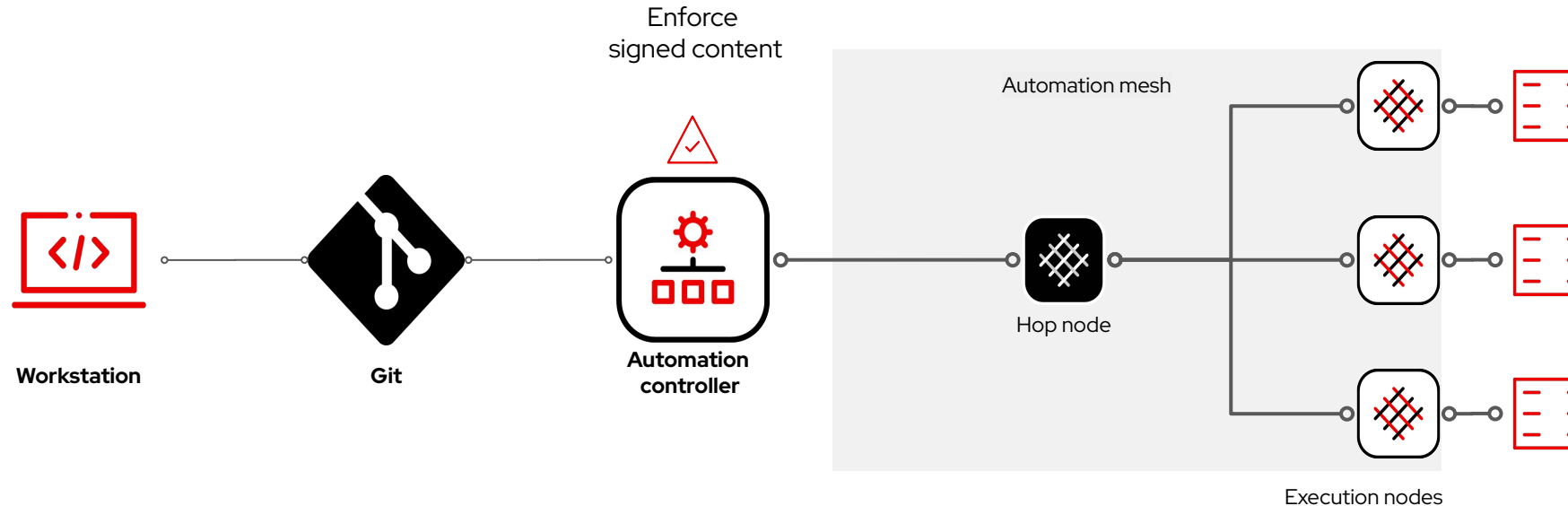
# Execution Environment signing service

- Signing in Automation Hub is based on GPG
- Signing service holds the GPG key and the signing script
- Signing service performs signing on execution environment/container image and adds the signature to the image itself



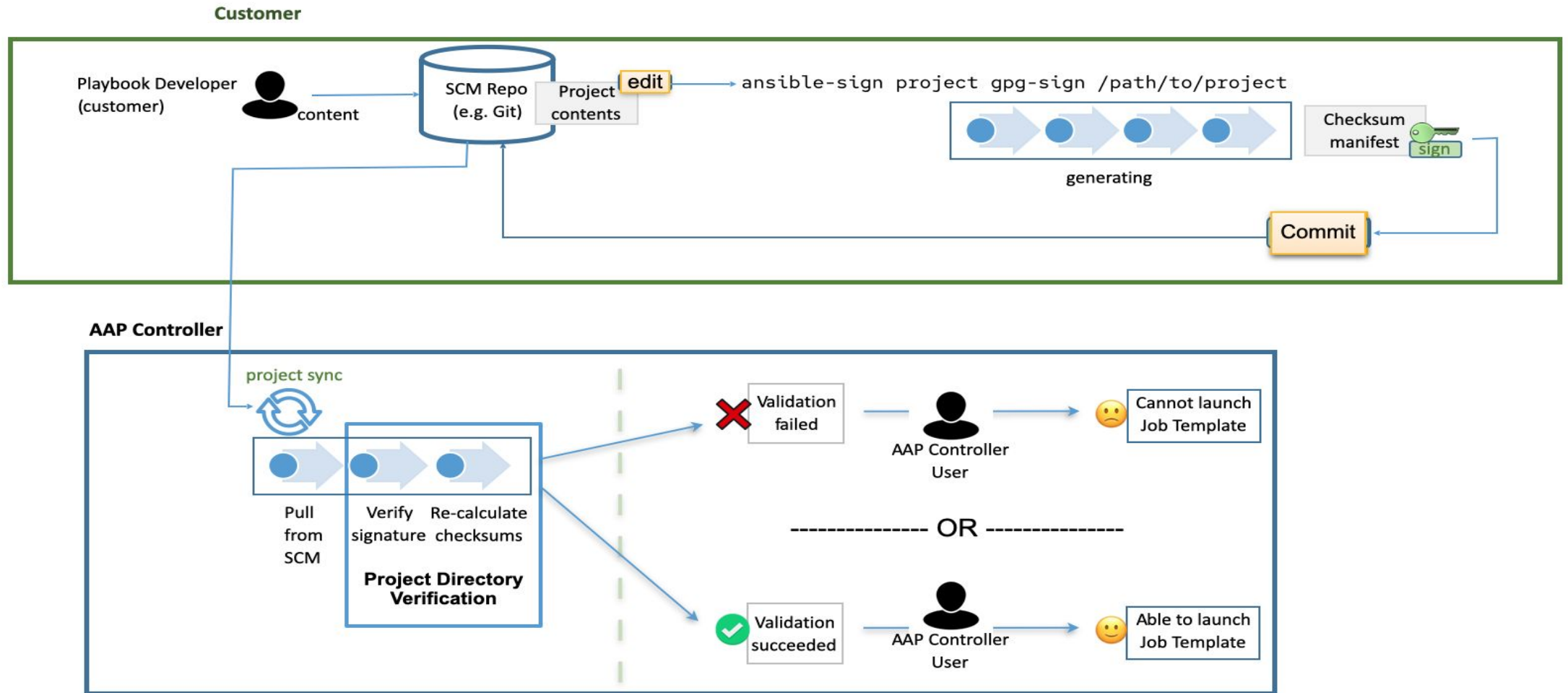
# Project signing and verification in Automation Controller

# Project signing in six steps



- 1 Create GPG key pair
- 2 Create an ASC file (armored ASCII)
- 3 Create a MANIFEST.in for your Git project
- 4 Use `ansible-sign` utility to create signature for the project
- 5 Create a GPG credential in Automation Controller
- 6 Sync Project (will be enforced!)

# Project signing workflow





# Project signing in Automation Controller

Projects **Create New Project**

Name \* Signed Project

Description

Organization \* Default

Execution Environment

Source Control Type \* Git

Content Signature Validation Credential \* ansible-sign

Type Details

Source Control URL \* https://gitea:8443/student/ansible-sign-demo.git

Source Control Branch/Tag/Commit

Source Control Credential

Options

Clean  Delete  Track submodules  Update Revision on Launch  Allow Branch Override

Save Cancel

**Add GPG key to validate project**

Signed Project Successful Plays 3 Tasks 9 Hosts 1 Elapsed 00:00:05

Stdout

```
0
1 PLAY [Update source tree if necessary] ***** 20:07:56
2
3 TASK [update project using git] ***** 20:07:56
4 changed: [localhost]
5
6 TASK [Set the git repository version] ***** 20:07:57
7 ok: [localhost]
8
9 TASK [Repository Version] ***** 20:07:57
10 ok: [localhost] => {
11   "msg": "Repository Version fe4a86fc402faa651263d2b3e6637683eb2daf01"
12 }
13
14 PLAY [Perform project signature/checksum verification] ***** 20:07:57
15
16 TASK [Verify project content using GPG signature] ***** 20:07:57
17 ok: [localhost]
18
19 TASK [Verify project content against checksum manifest] ***** 20:07:57
20 ok: [localhost]
21
22 PLAY [Install content with ansible-galaxy command if necessary] ***** 20:07:57
23
```

**Project sync job will do the GPG verification**

# Resources

- **Self-paced Labs**

- [Signing in Private Automation Hub](#)
- [Project signing in automation controller](#)

- **Blogs**

- [Digitally signing Ansible Content Collections using private automation hub](#)
- [Project signing and verification](#)

- **Documentation**

- [Collections and content signing in private automation hub](#)
- [Project Signing and Verification](#)
- [Image Signature Verification](#)

Session: 17:25 - 17:55



[red.ht/rhsc24-de-s8](https://red.ht/rhsc24-de-s8)

# Jetzt Session bewerten!

Einfach QR-Code  
scannen, Session  
wählen und bewerten.  
**Vielen Dank!**

Red Hat  
**Summit**

**Connect**

Thank you



[linkedin.com/company/red-hat](https://www.linkedin.com/company/red-hat)



[facebook.com/redhatinc](https://www.facebook.com/redhatinc)



[youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)



[twitter.com/RedHat](https://twitter.com/RedHat)