Pam-Weblogin

Leveraging your federated identity to authorize SSH sessions

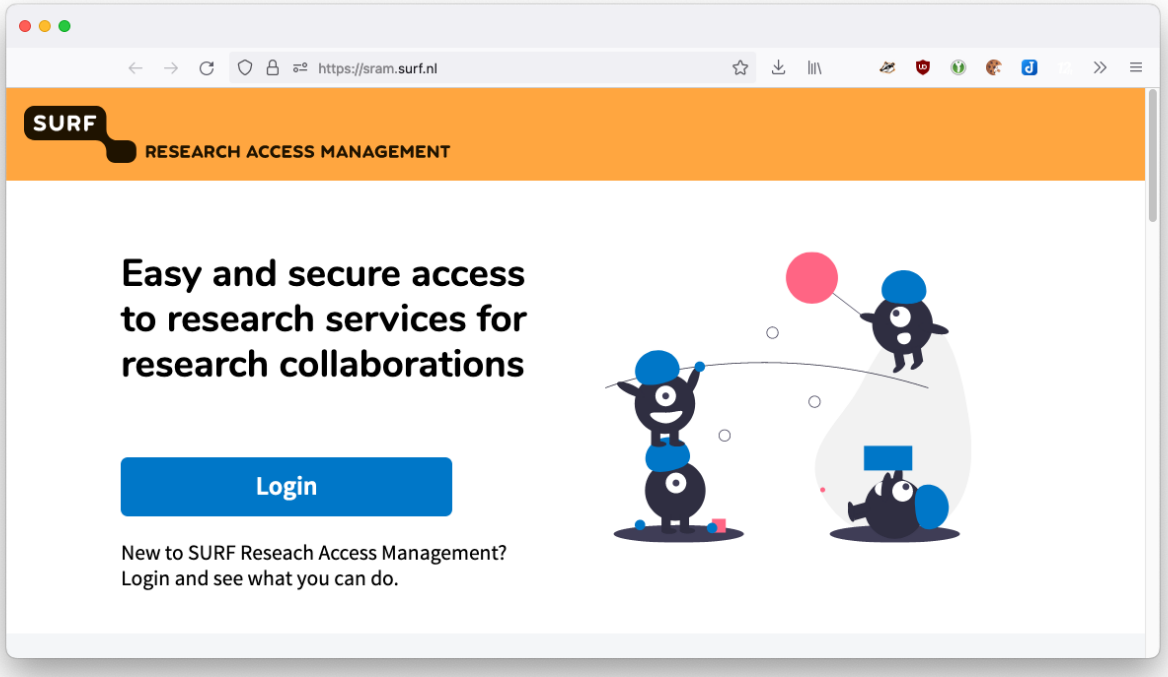
Martin van Es <martin.vanes@surf.nl>

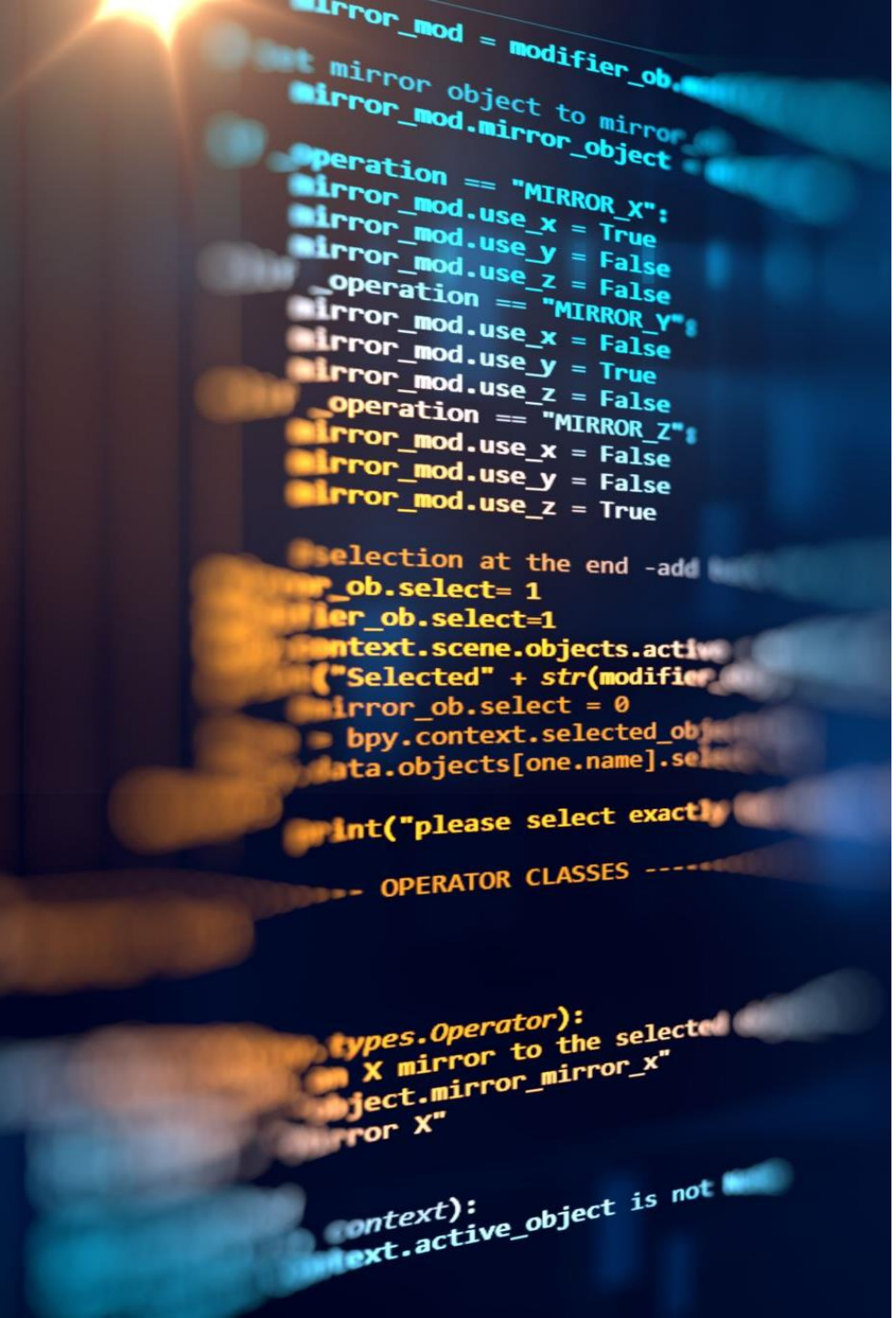
Bas Zoetekouw <bas.zoetekouw@surf.nl>

Background

SURF Research Access Management
https://sram.surf.nl/

- User friendly
- No credential storage



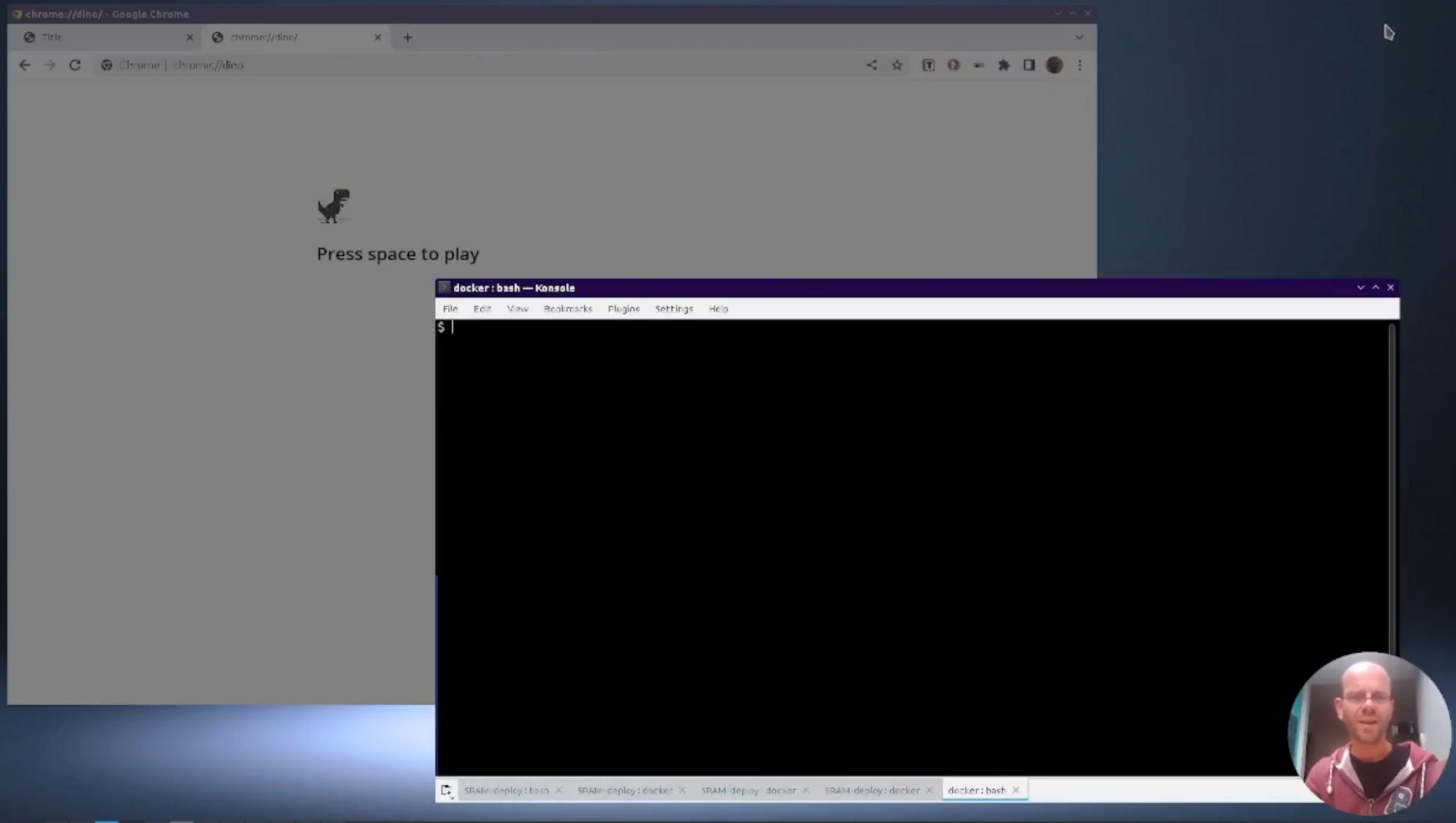


Solution

Pam-Weblogin

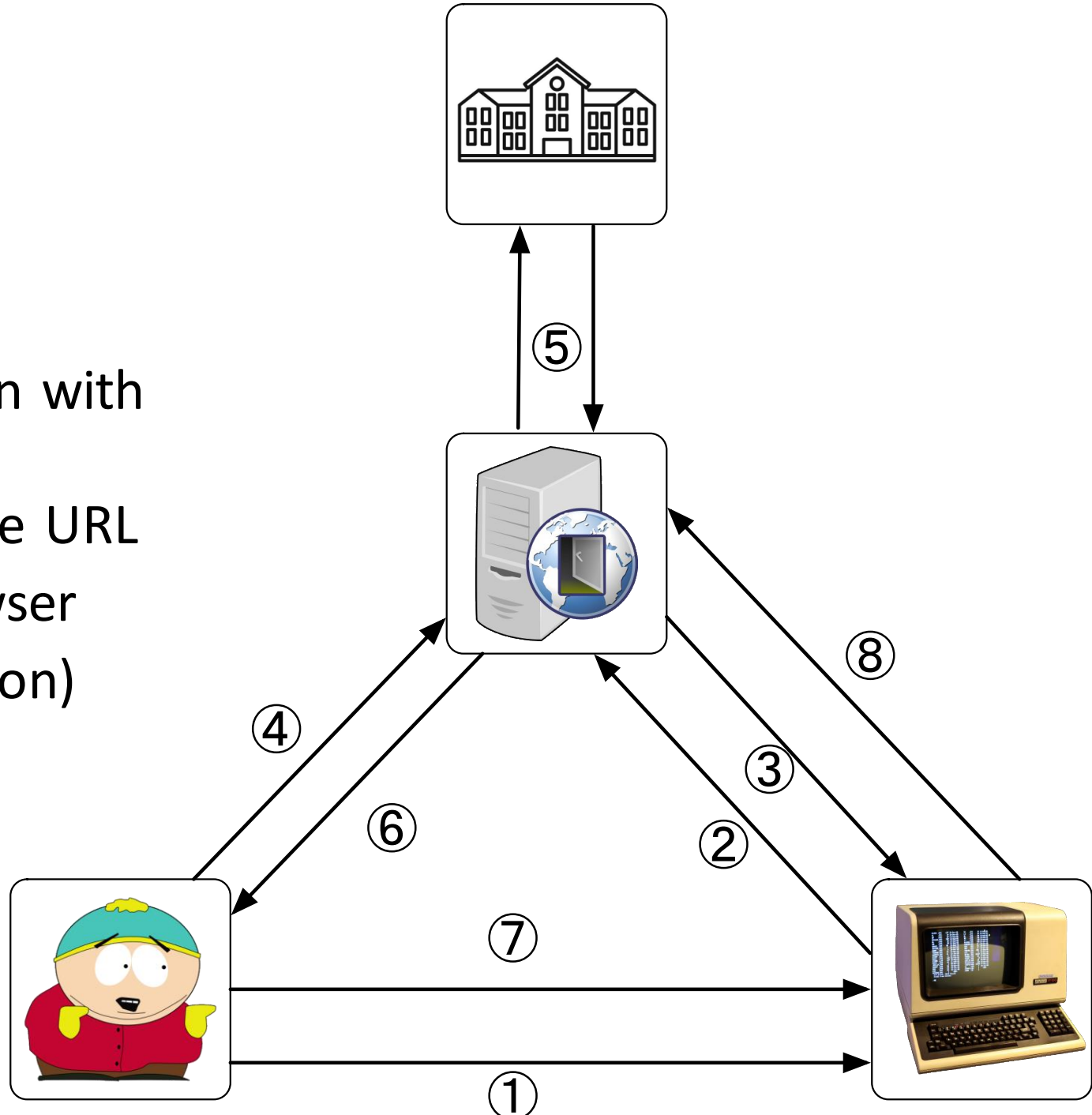
- User connects as usual
  (no custom clients, no configuration)
- Server asks user to visit URL
- User logs on in their webbrowser
- Web page shows a verification code
- User enters verification code in original session
- Login continues

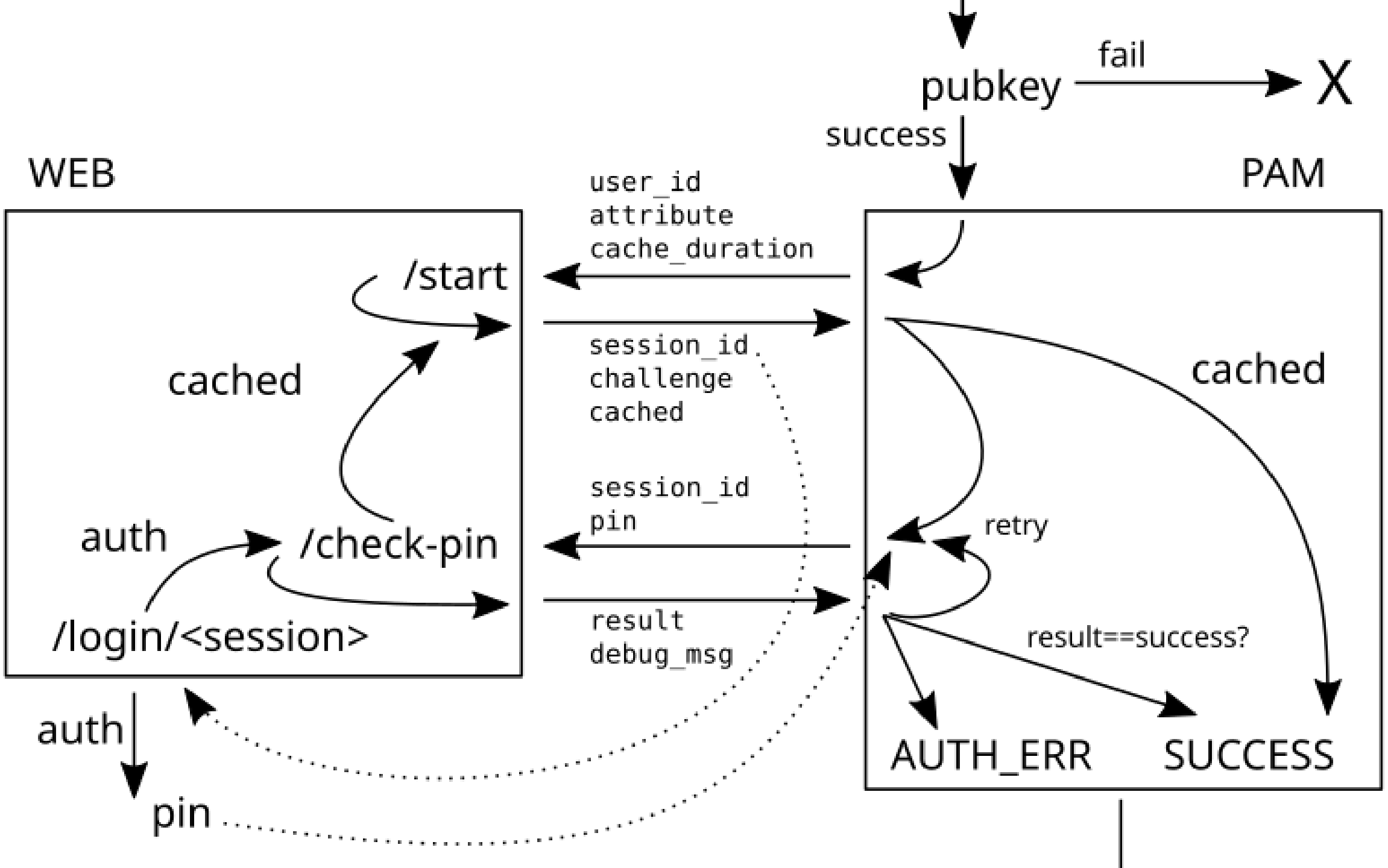
Demo time!


chrome://dino/ - Google Chrome
Title
chrome://dino/
Chrome | chrome://dino
Press space to play
docker : bash — Konsole
File Edit View Bookmarks Plugins Settings Help
$
docker : bash

In detail

1. User starts terminal session
2. Terminal server set up session with Weblogin server
3. Weblogin server sends unique URL
4. User clicks url; opens in browser
5. User logs in (e.g., via federation)
6. Weblogin shows pin to user
7. User enters pin in terminal
8. Terminal verifies pin




pubkey
fail
X
success
WEB
PAM
user_id
attribute
cache_duration
/start
cached
session_id
challenge
cached
cached
session_id
pin
retry
auth
/check-pin
/login/<session>
result
debug_msg
result==success?
auth
AUTH_ERR
SUCCESS
pin

Requirements

- Generic for any PAM-authentication
- Needs fully implemented PAM stack (conversation)
- The PAM module must be compiled, installed and configured on the server. This could be packaged.
- Existing user equal to one of the internal SBS user attributes

USPs

- Generic PAM implementation (conversation required)
- Vanilla clients and servers
- Device binding guaranteed
- Authorization bound to personal IdP login or session
- Can be used a first or second factor
- MFA can be enforced in the SAML or OIDC flow
- Authentication only works as long as the user has valid credentials or a session at the IdP

Overview

Does the solution mitigate sharing of SSH keys?	✓
What are the client requirements and supported platforms?	PAM stack
What are the SSH server requirements and does the solution require additional software beyond SSH server?	
Does the solution allow for non-interactive client logins?	✗
Does the solution allow for delegation?	✗
What requirements are put on the incoming federated identity?	username==claim
How is provisioning towards the SSH server set up?	out of scope
How does revocation work?	authN fails
Does the setup allow for MFA?	✓

Check it out!

https://github.com/SURFscz/pam-weblogin