Passwordless authentication in GDM

Joan Torres Lopez <joantolo@redhat.com>

Iker Pedrosa <ipedrosa@redhat.com>

Who are we?

Iker Pedrosa

Software Engineer at Red Hat

Focus on Identity Management

- SSSD
- shadow
- Linux-PAM

ipedrosa@redhat.com

ikerpedrosa

Who are we?

Joan Torres Lopez

Software Engineer at Red Hat

GNOME desktop

joantolo@redhat.com

gitlab.gnome.org/joantolo

Agenda

1. Passwordless authentication
2. GDM authentication
3. Limitations
4. Solution
5. Conclusion

1. Passwordless authentication

What is passwordless?

- A way to authenticate a user without using a password
- Usually involves MFA and SSO
- It strengthens security and improves user experience

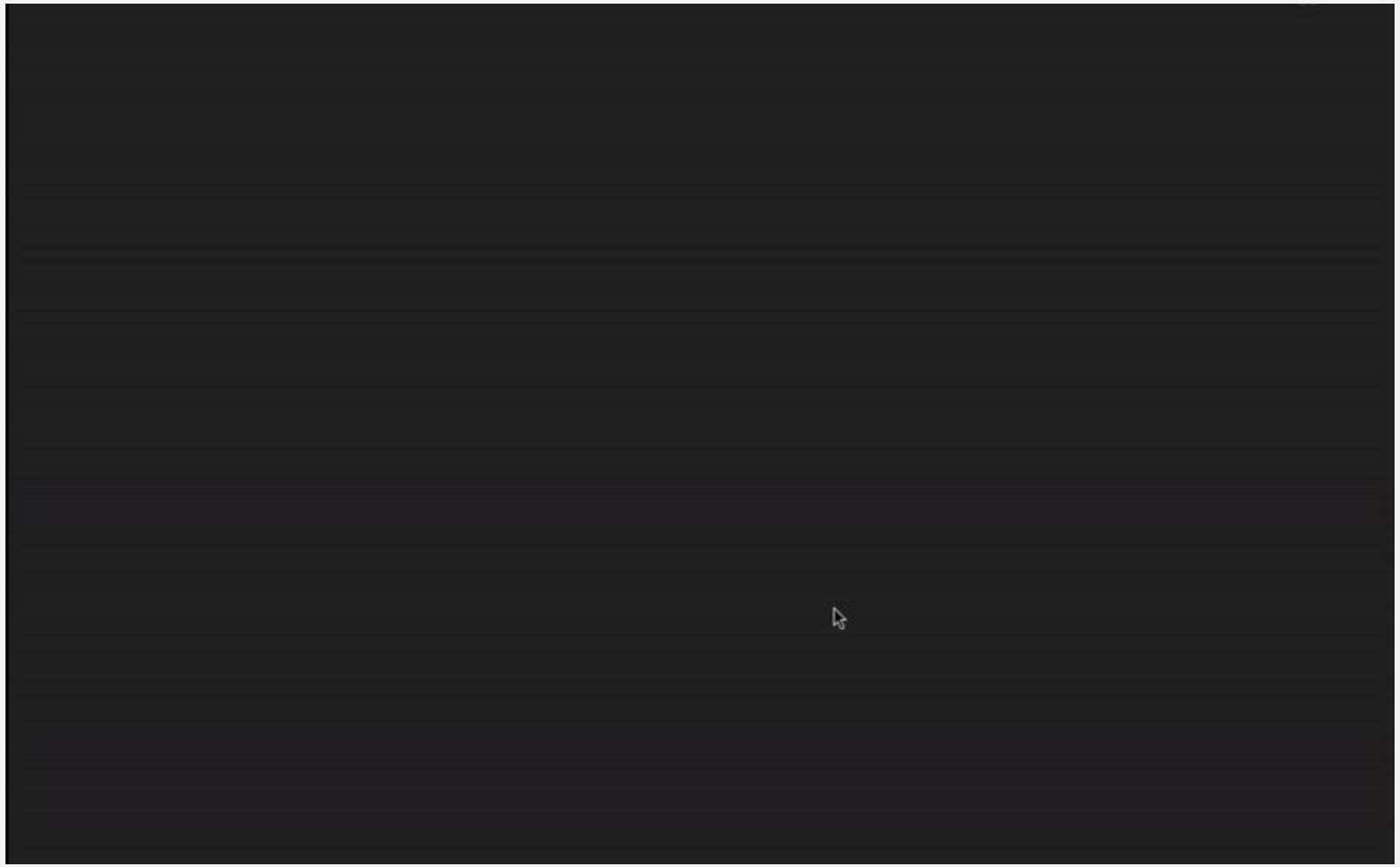
Passwordless mechanisms

Available mechanisms for centrally managed users in FreeIPA and SSSD

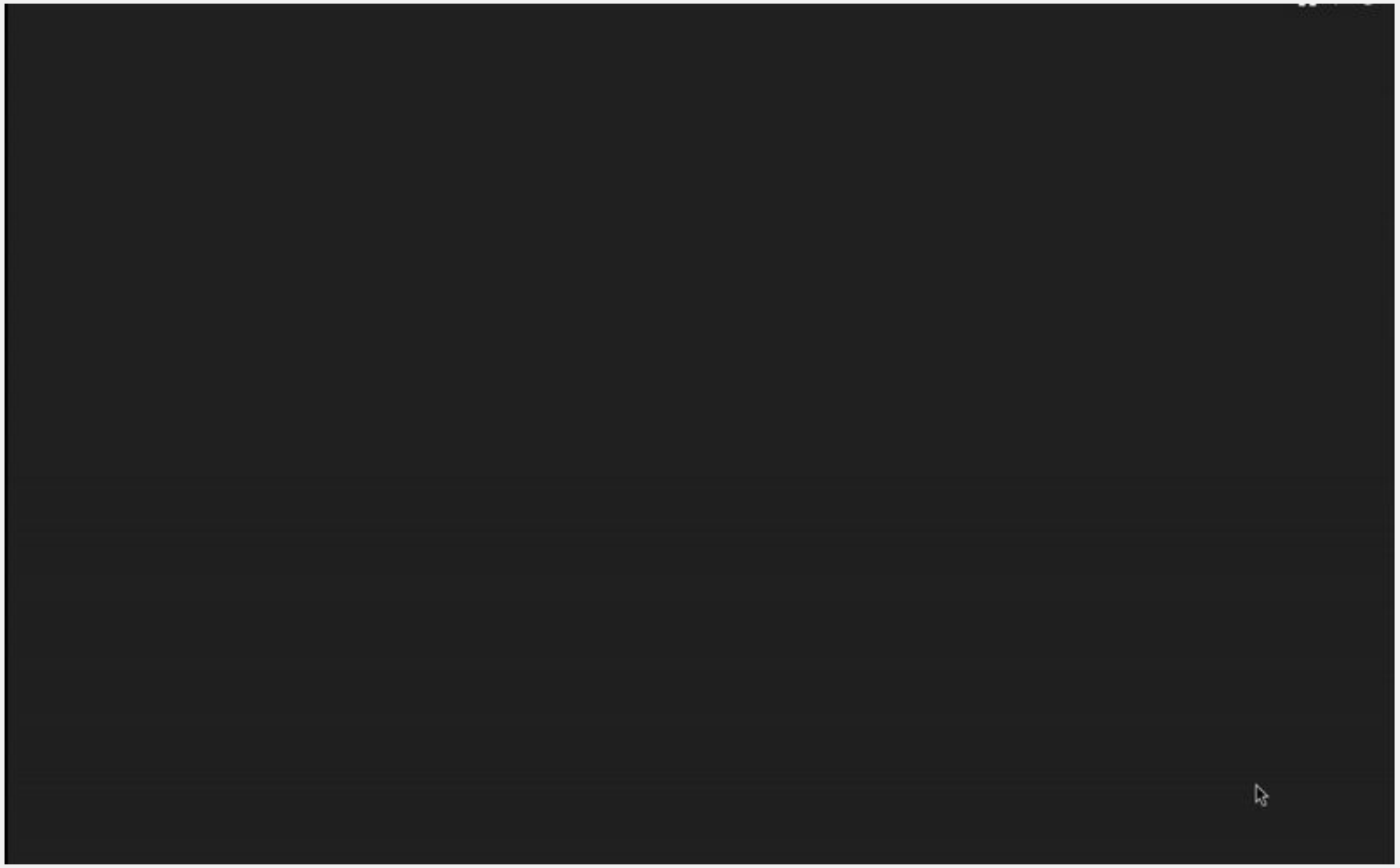
- Passkey
- Smartcard
- External Identity Provider

2. GDM authentication

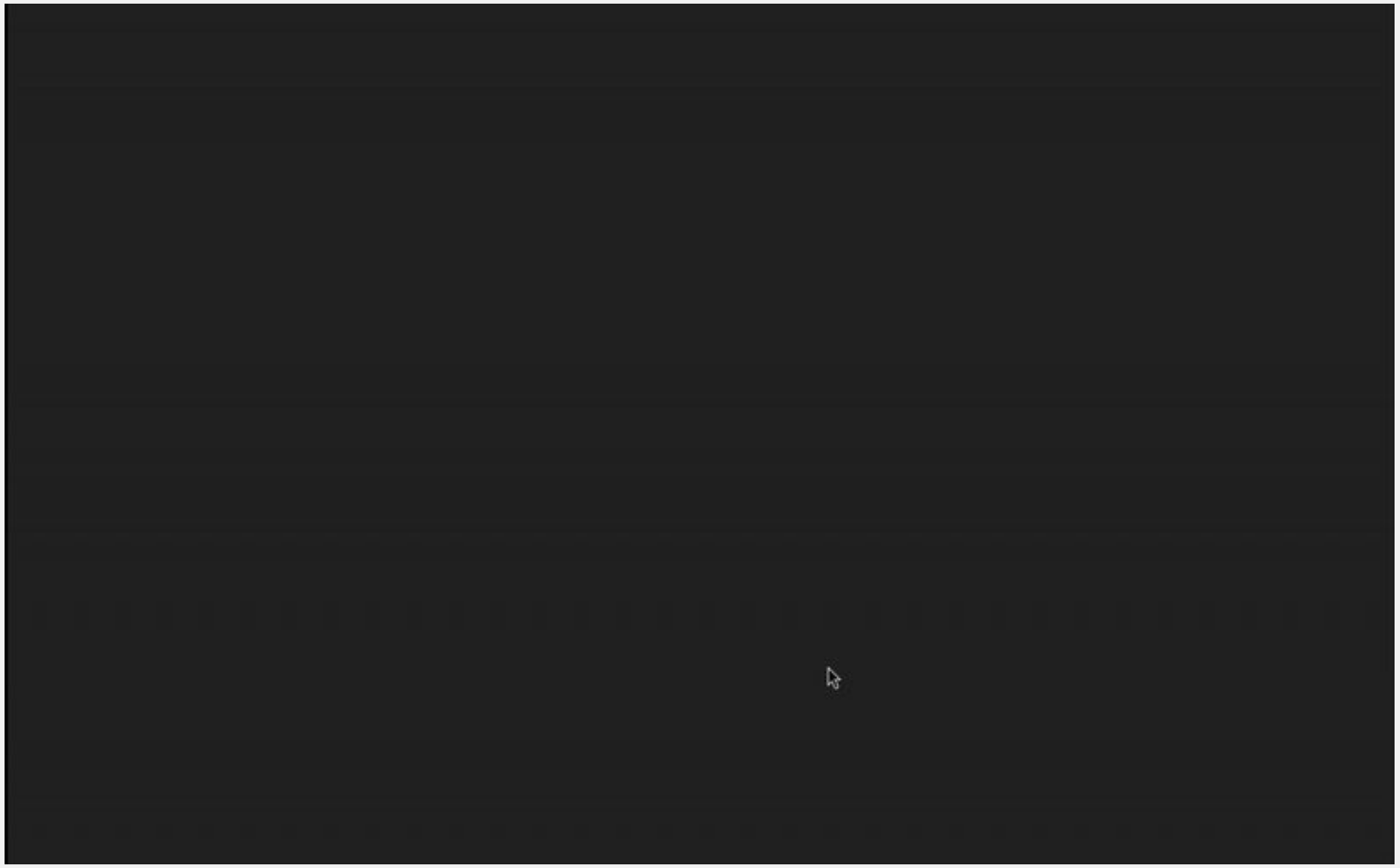
Password authentication



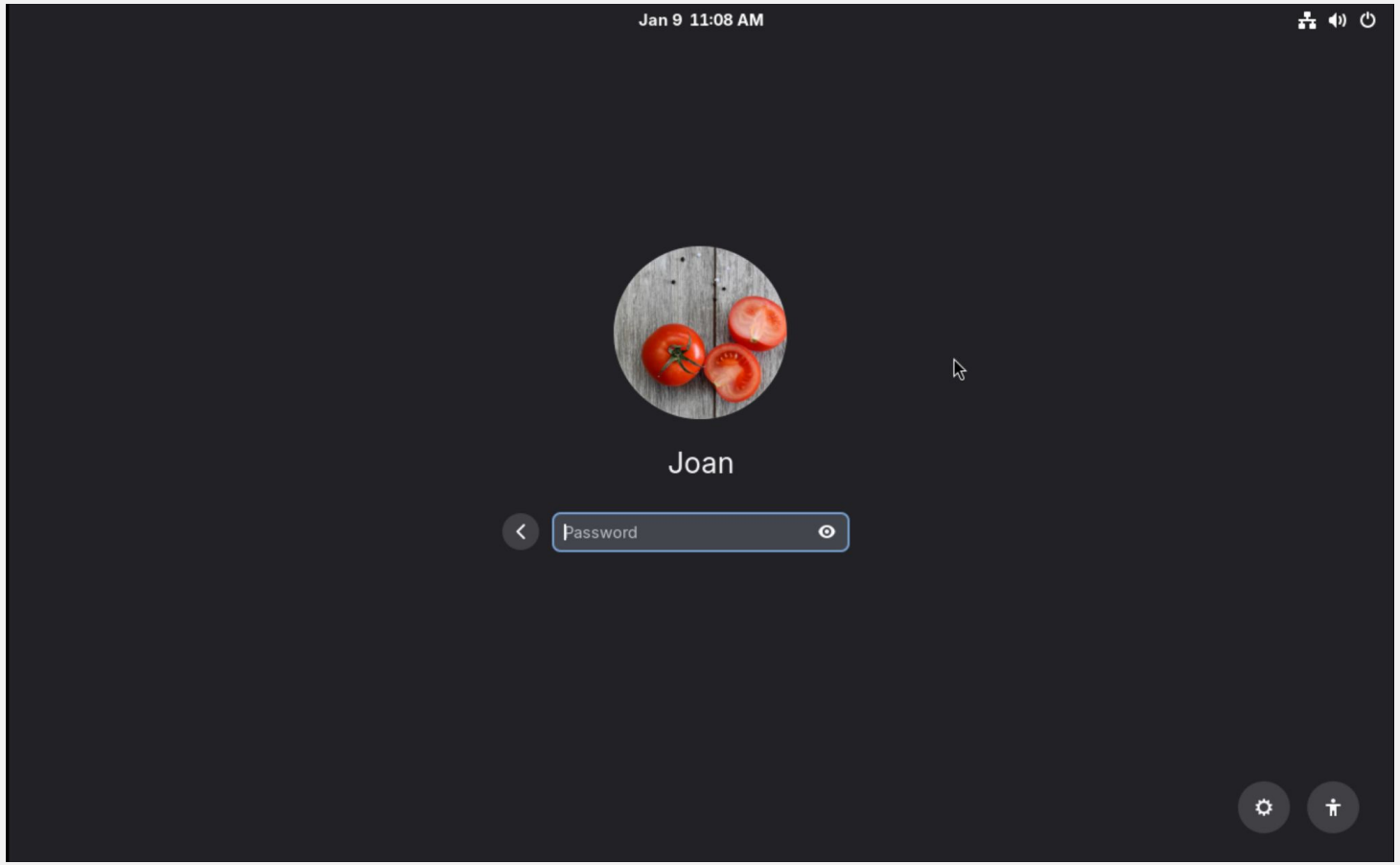
Smartcard authentication



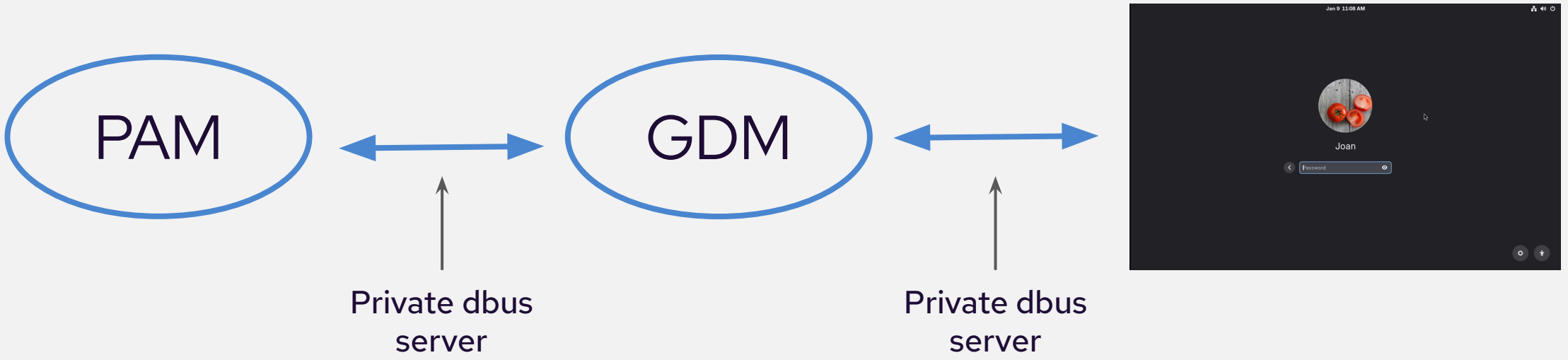
Fingerprint authentication



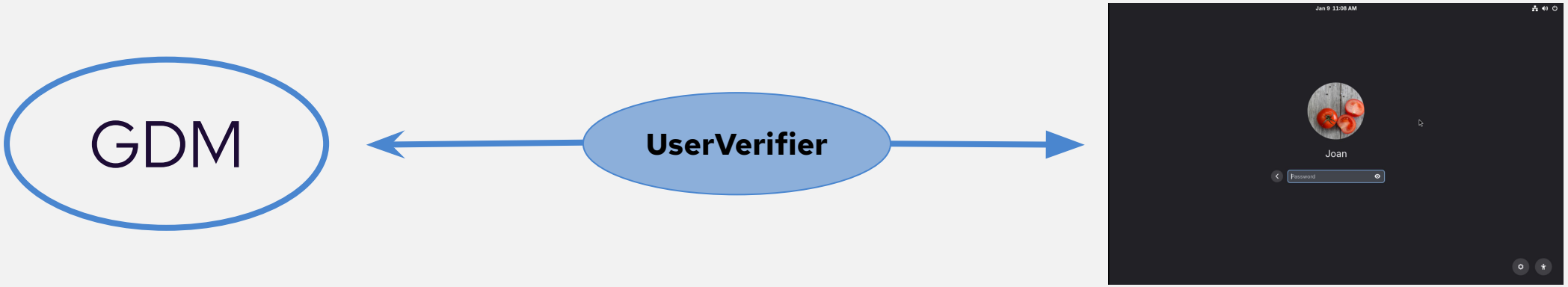
How’s authentication done?



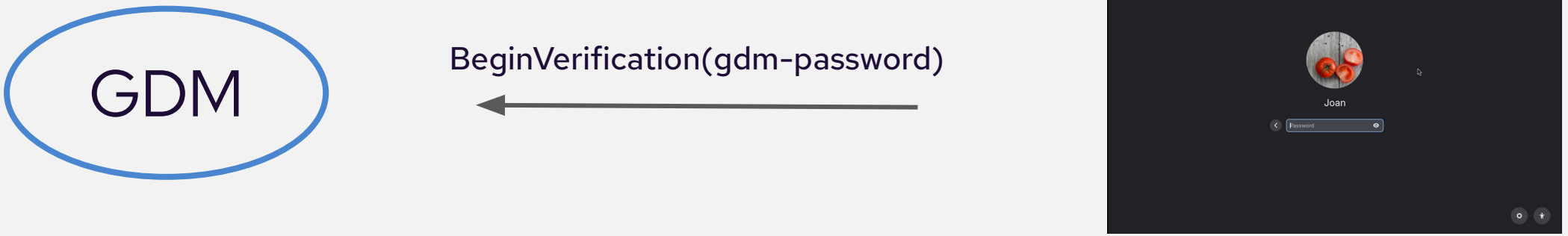
How’s authentication done?



How’s authentication done?

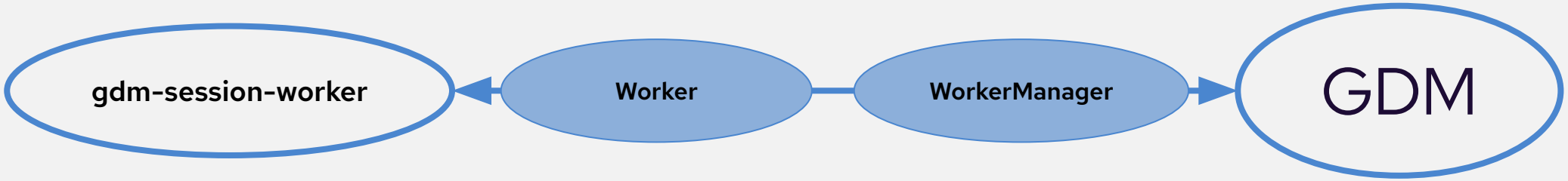


How’s authentication done?

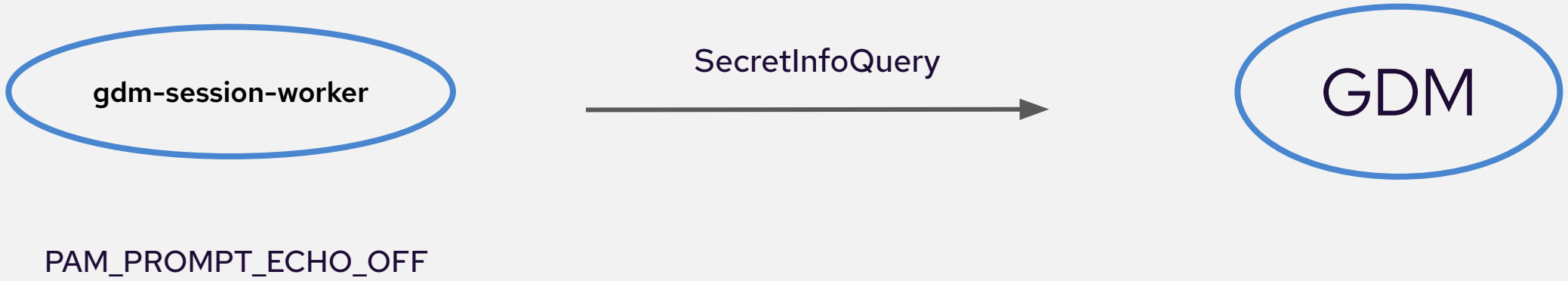


How’s authentication done?

How’s authentication done?



How’s authentication done?



3. Limitations

Problem statement

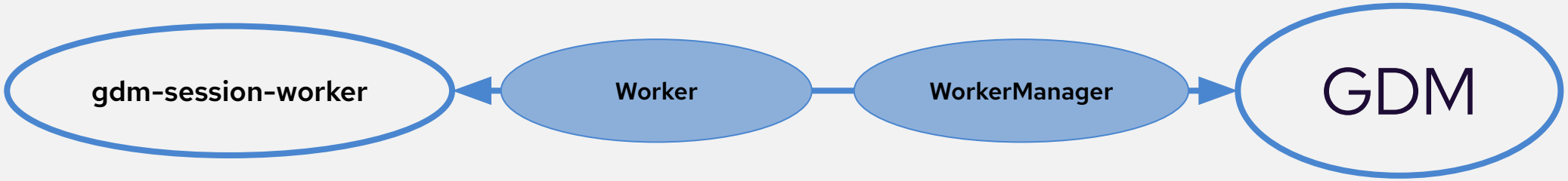
- Conversation very rigid (only supports text exchange)
- Doesn’t support “Touch device” or “WebView” PAM requests
- Can’t advertise available authentication methods
- Poor UX experience
- No ZTA support

4. The solution

New PAM extension

- With msg_type = PAM_BINARY_PROMPT
- New extensions to messages
- New extension: “CustomJSON”

New PAM extension



New PAM extension

New PAM extension

- Supported by sssd and authd
- sssd: **gdm-switchable-auth**
- authd: **gdm-authd**

JSON message format

- Request

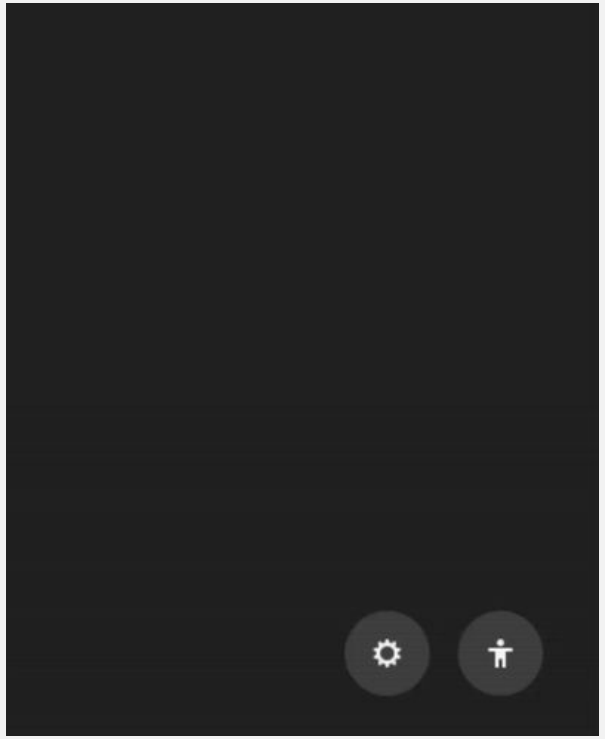
```
{
  "authSelection": {
    "mechanisms": {
      "$mech1": {
        "name": "$name1",
        "role": "$role1",
        "msg1": "$msg1"
      },
      "$mech2": {
        "name": "$name2",
        "role": "$role2",
        "msg1": "$msg2",
        "msg2": "$msg3"
      }
    }
  }
}
```

- Reply

```
{
  "authSelection": {
    "status": "$status",
    "mech": {
      "data1": "$data1",
      "data2": "$data2"
    }
  }
}
```

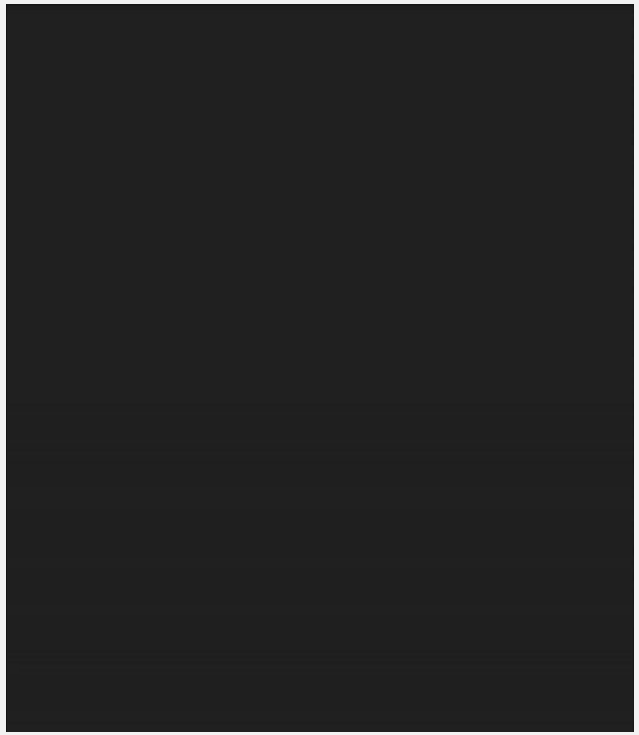
GDM changes

- Mechanisms are selectable



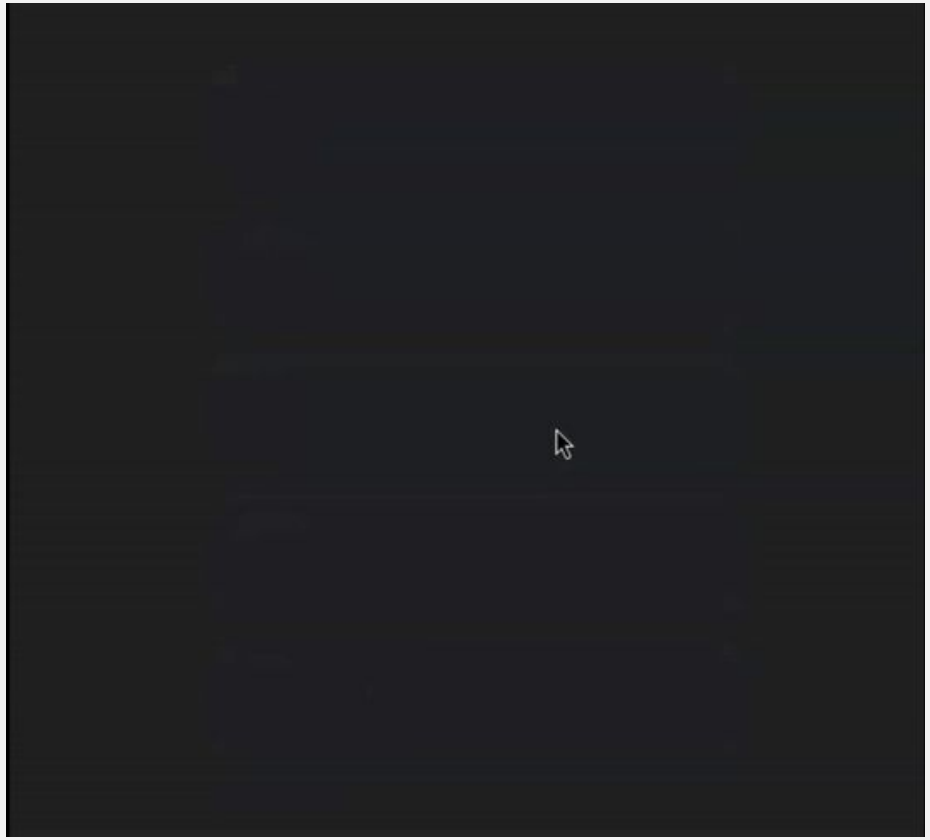
GDM changes

- Smartcard UI updated



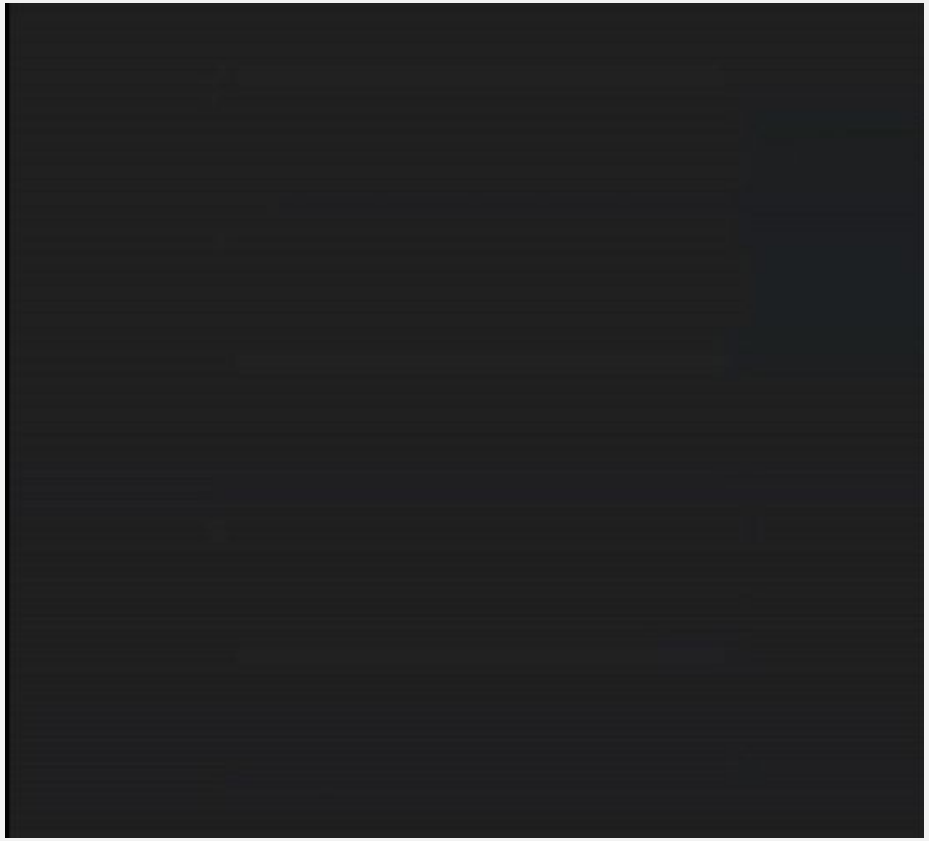
GDM changes

- New Passkey mechanism



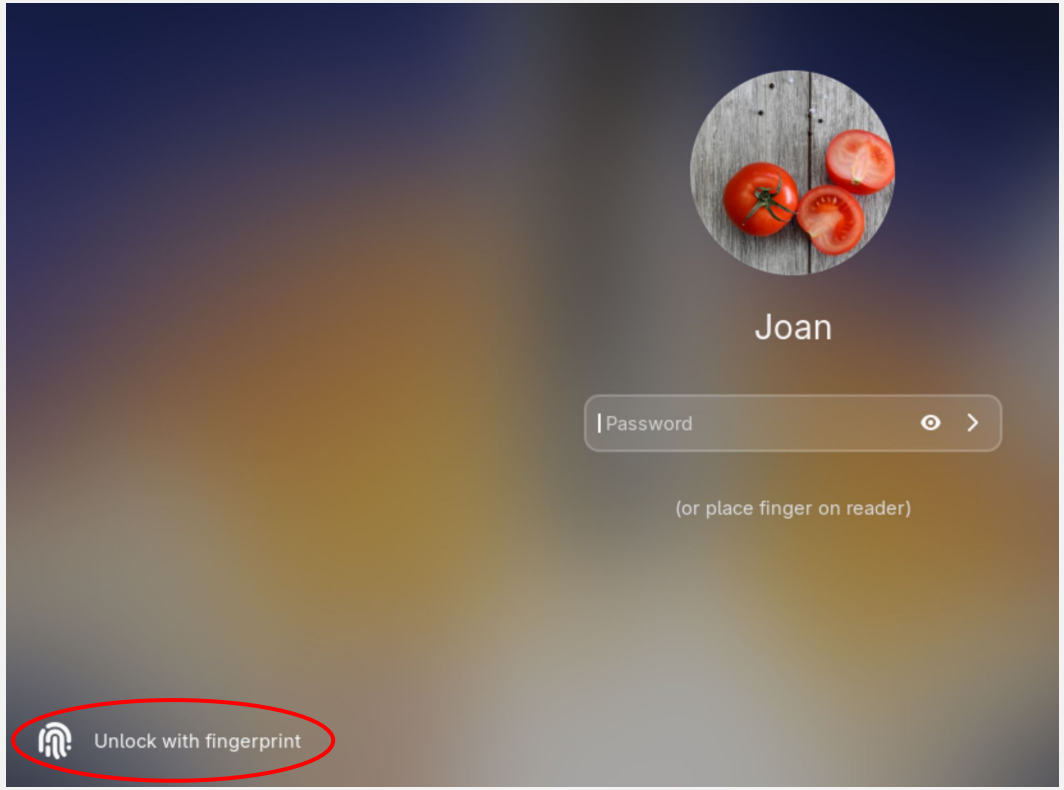
GDM changes

- New Web Login mechanism



GDM changes

- Fingerprint only on lockscreen



Live demo

5. Conclusion

Feature availability

- sssd 2.12.0
- GNOME 50 (tentative) <- MR#3212 and MR#185

Future enhancements

- Embedded webview
- PAM conversation through fd
- Move GDM into systemd (live discussion)

Reference links

- SSSD-GDM interface design
- Blog post: Enhancing PAM communication
- COPR repository

Credits

- Ray Strode <rstrode@redhat.com>
- Marco Trevisan (Treviño) <mail@3v1n0.net>

Thank you!