SSH – Bad Habits and Their Solutions

- **mag. Sergej Rožman**; Abakus plus d.o.o.

- The latest version of this document is available at:

  http://www.abakus.si/


CYBERCRIME

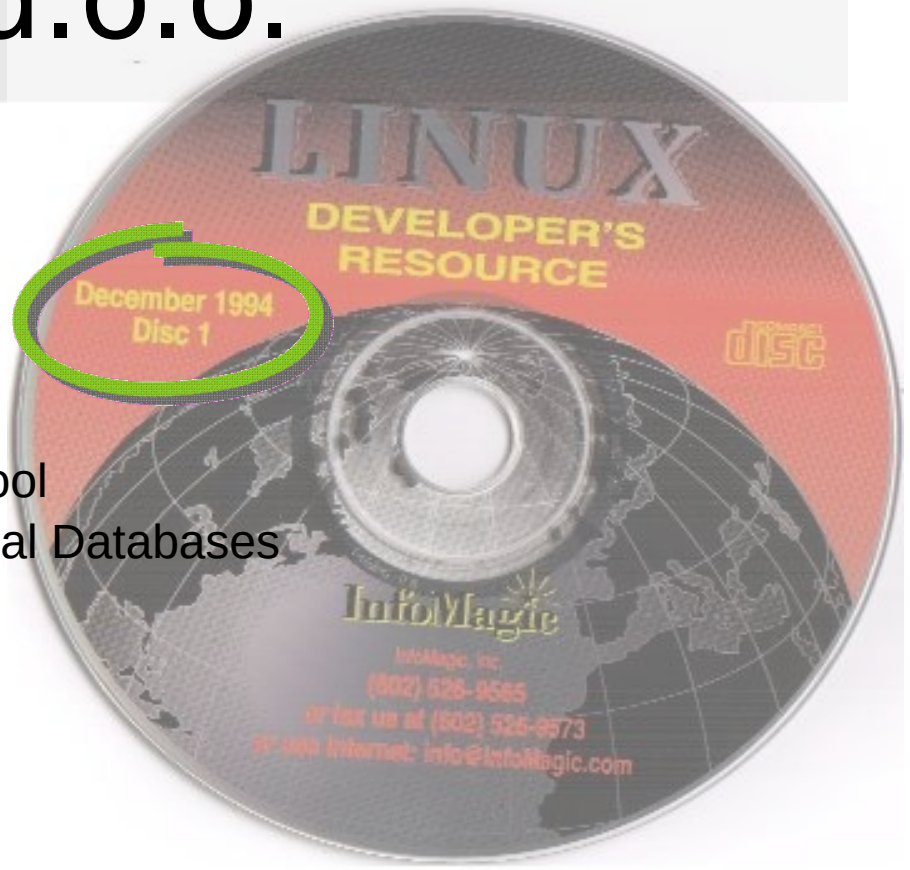
SSH – Bad habits and their solutions

mag. Sergej Rožman

sergej.rozman@abakus.si

Make IT 2025

Abakus plus d.o.o.



History

- since 1992, ~20 employees

Applications:

- ARBITER – the ultimate tool in audit trailing
- APPM – Abakus Plus Performance Monitoring Tool
- DejaVu - High Performance Architecture for Virtual Databases

Services:

- DBA, OS administration , programming (Oracle)

Infrastructure:

- servers, SAN storage, UPS, firewalls, backup servers, virtualization

Skills & Experience:

- from 1995 GNU/Linux ***(~30 years of experience !)***
- Oracle on GNU/Linux: since RDBMS 7.1.5 & Forms 3.0 ***(before Oracle !)***
- **~35 years of experience with High-Availability !**

Customers


Gorenjska Banka
GENERALI Zavarovalnica
Ljubljana Airport
Iskra
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO
NOVA BANKA
MILENIJUM OSIGURANJE
DRINA OSIGURANJE
MM KARTON
KONTROLA ZRAČNEGA PROMETA SLOVENIJE
Hidria
Mestna občina Ljubljana
skbbanka otp group
PH
triglav
GOODYEAR
TRELLEBORG
UNIVERZITETNA PSIHIATRIČNA KLINIKA LJUBLJANA
University Psychiatric Clinic Ljubljana
BANKA SLOVENIJE
Blubit
SAVA INFOND
PRVA
ELES
Фонд здравственог осигурања Републике Српске
NLB Vita
Življenjska zavarovalnica
G96
EKDIS
CENTROSINERGIJA
SAVA HOTELS & RESORTS
terme čatež
NLB Skladi
Mercator
MAGNETIK
MERKUR
SPL d.d.
ZAVOD ZA ŠPORT RS PLANICA
editel
INFOTRANS
LASERLINE
studio ritem
PRONET CHOOSE THE FUTURE
hit alpinea Kranjska Gora
ORACLE
ROS d.o.o.
sij acroni
ANDRITZ
jata emona LJUBLJANA
ADRIA ANKARAN HOTEL & RESORT

What do we want to achieve?

We manage 1000+ Physical and Virtual Servers Across Multiple Client Environments

- Security hardening at scale
- Efficient user lifecycle management *(the server must be self-sufficient)*
- Audit trail and session logging *(optional but desirable)*

SSH – Secure Shell

The ubiquitous de facto standard

- Traditionally included on Linux (Unix) systems

Windows

- SSH client included since Windows 10 version 1803 and Windows Server 2019
- SSH server as an Optional feature

- Mostly included in embedded systems (routers, switches, firewalls, NAS, SAN, ...)

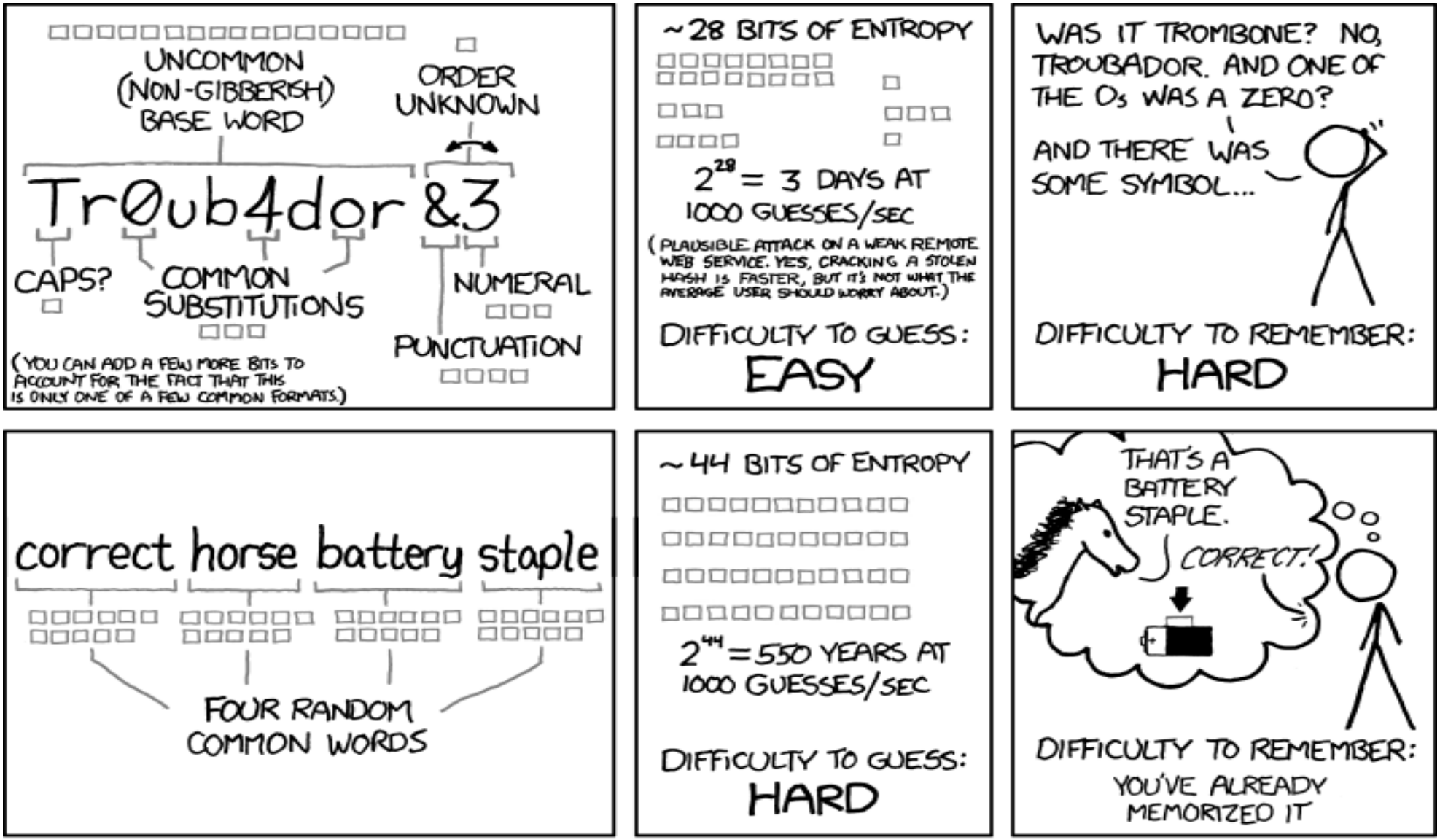
Password Authentication

Problems:

- Weaker security
  - Brute force attack
  - Password transfers over the line *(although encrypted)*
  - Reusing/sharing passwords
- No MFA
- Difficult to enforce policies
- Less automation friendly *(scripts)*
- No user management

Abakus
As na disku.

Password Threats



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

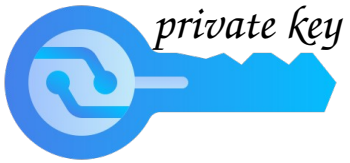
SSH Public-key Authentication

Pros:

- Simplicity
- Familiarity
- **Private key never leaves the client**

Cons:

- Difficult to enforce policies
- No user management
- No MFA



SSH Public Keys

- Generating a user keypair

```
ssh-keygen -t ed25519 -C "user@example"
```

- Produces two files:

```
# private key
~/.ssh/id_ed25519

# public key
~/.ssh/id_ed25519.pub
```

- Appending the public key to the remote site into the users’s authorized_keys

```
cat ~/.ssh/id_ed25519.pub >> ~/.ssh/authorized_keys
```

SSH Public-key User Authentication

client

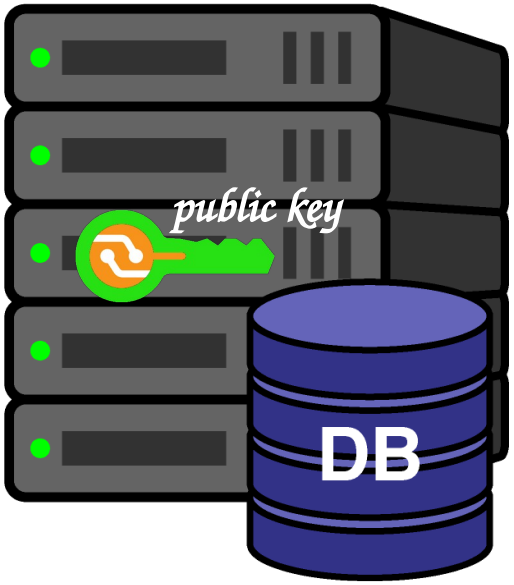
server

initiate SSH connection

send some challenge

ssh-agent signs the challenge

server verifies the signature

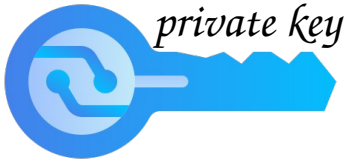


if the signature is valid, the client is authenticated

Abakus
As na disku.

Digital Certificate

- CA guarantees the authenticity of the public key.
- Contains attributes



X.509 vs SSH Certificate

SSH Certificate Config

- Enter the CA public key

```
/etc/ssh/sshd_config.d/ssh_user_ca_key.pub:

ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNwHkLXc
QJAThObgJlYSEhkQ1jtU0MaTs7gnwMAmnxYGznaDt5F/YKzScWvZ/UgjhD4HCSFo+tVFBhek7QoA2I4=
```

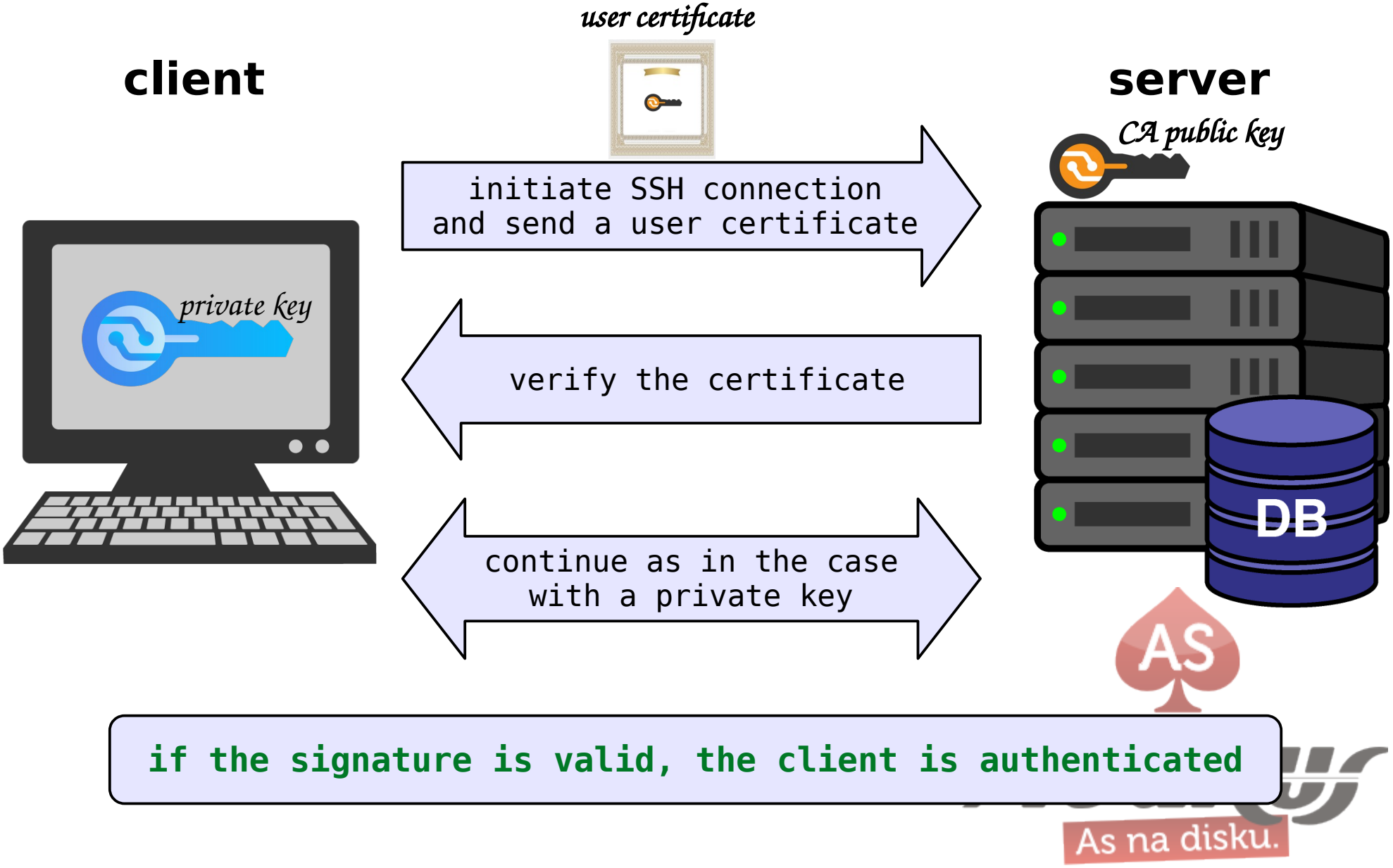
- into the sshd configuration

```
/etc/ssh/sshd_config:

# This is the CA's public key for authenticating user certificates:
TrustedUserCAKeys /etc/ssh/sshd_config.d/ssh_user_ca_key.pub
```

Abakus
As na disku.

SSH User Certificate Authentication Sequence



SSH Certificates Using SSH Tools

- Generate CA keypair

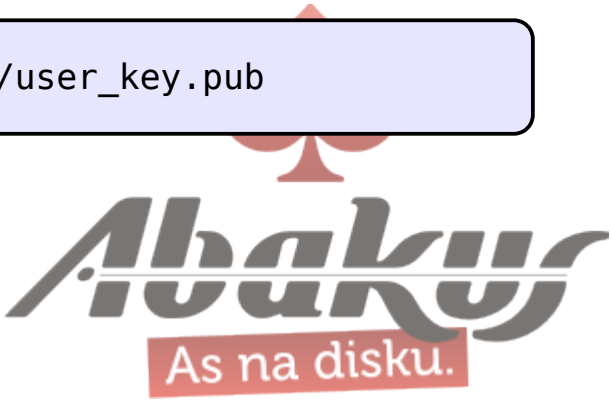
```
ssh-keygen -f ~/.ssh/ssh_ca -t rsa -b 4096 -C "SSH CA"
```

- Generate a user keypair

```
ssh-keygen -f ~/.ssh/user_key -t ed25519 -C "user@example"
```

- Sign the user’s public key with the CA

```
ssh-keygen -s ~/.ssh/ssh_ca -I ID -n username -V +52w ~/.ssh/user_key.pub
```



SSH Certificate

- Inspect the user certificate

```
ssh-keygen -L -f ~/.ssh/user_key-cert.pub
/root/.ssh/test/user_key-cert.pub:
        Type: ssh-ed25519-cert-v01@openssh.com user certificate
        Public key: ED25519-CERT SHA256:K16ar6fqhPvxjdxsQaXSk49JKN4+4sgbUZ/DILkzHBg
        Signing CA: RSA SHA256:fMazeIL5G3La8vRy///Hz7zMj+Zmyhhv7VPwzSYtOGk
          (using rsa-sha2-512)
        Key ID: "ID"
        Serial: 0
        Valid: from 2025-05-08T14:53:00 to 2026-05-07T14:54:22
        Principals:
                janez
        Critical Options: (none)
        Extensions:
                permit-X11-forwarding
                permit-agent-forwarding
                permit-port-forwarding
                permit-pty
                permit-user-rc
```

Introducing Smallstep

https://smallstep.com/product/ssh/

- Open-source CA (SSH and X.509 certificates)

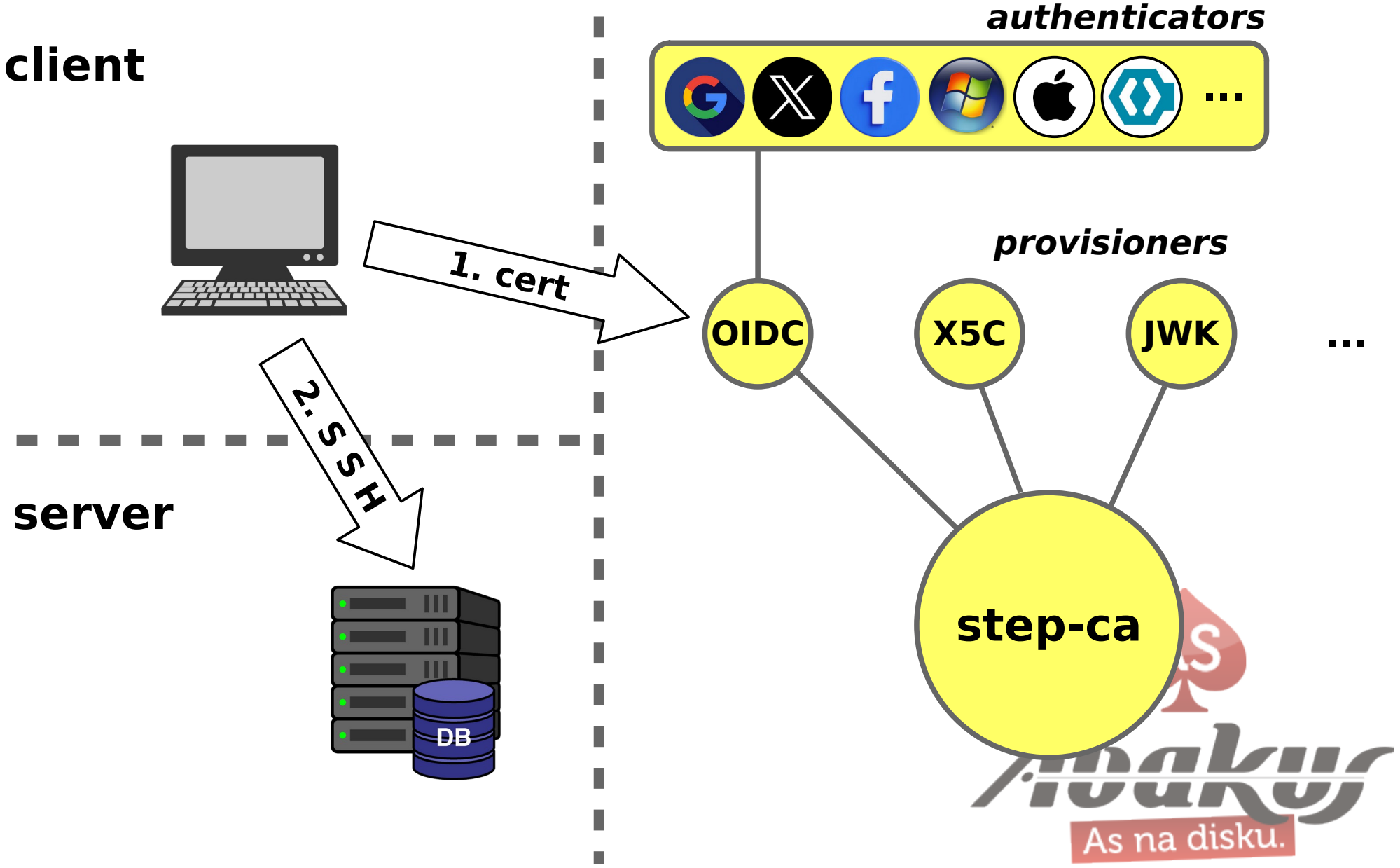
Server – step-ca

- On-premises or
- CA as a service from the cloud

Client – step-cli

- Linux
- Windows
- MacOS

SSH log in


client
server
authenticators
...
provisioners
OIDC
X5C
JWK
...
1. cert
2. SSH
DB
step-ca
Abaku
As na disku.

SSH Certificates Using step-cli

- Generate a user keypair and certificate

```
step ssh certificate ID ~/.ssh/user_key
```

- Generate a private key, certificate and add them to the ssh-agent

```
step ssh login username@host.si
```

- Automatic integration into the SSH client

```
~/.ssh/config:

Match exec "step ssh check-host %h"
        User $USER
        ProxyCommand step ssh proxycommand %r %h %p --provisioner "Google"
```

SSH Certificate

- Inspect the user certificate using »step ssh inspect«

```
step ssh inspect ~/.ssh/user_key-cert.pub
/root/.ssh/test/user_key-cert.pub:
        Type: ecdsa-sha2-nistp256-cert-v01@openssh.com user certificate
        Public key: ECDSA-CERT SHA256:wEKh31hlxfhlJIhzVsLmdWVXJTtnvtAonRiJ/veCUmI
        Signing CA: ECDSA SHA256:urGP2m5XNO8OQu1z1a8G2TwkYFUekhcJUi5ZoSKhBpM
          (using ecdsa-sha2-nistp256)
        Key ID: "sergej@abakus.si"
        Serial: 1005835596821517067
        Valid: from 2025-05-26T13:50:58 to 2025-05-26T21:50:58
        Principals:
                sergej
                sergej@abakus.si
        Critical Options: (none)
        Extensions:
                permit-X11-forwarding
                permit-agent-forwarding
                permit-port-forwarding
                permit-pty
                permit-user-rc
```

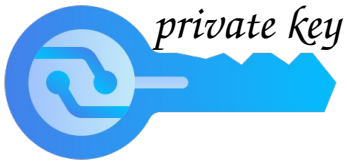
Certificate vs Public Key Authentication

Pros:

- Simplicity
- Familiarity
- **Private key never leaves the client**

Cons:

- Difficult to enforce policies
- No user management
- No MFA



User Management

First idea

- A user who has never been seen before but **has a valid certificate** wants to log in.


```
/etc/ssh/sshd_config:

# Script to be executed upon certificate authentication
AuthorizedPrincipalsCommand <script.name>
```

Access Denied

Authorisation denied for non-existent user

- The server does not run AuthorizedPrincipalsCommand if a user does not exist

Creating a User Account

First access to the system in two steps

- Log in to a proxy account using the user certificate to create a user account

- Log in to a user account

Improvements?

Ideas

- Patch ssh-server
  - Contribute to the improvement to the community
  - Asking ssh authors for improvement
- Something else

For the end – work in progress

Audit Trail – sshlog.com

- Monitor SSH access to servers and detect suspicious activity
- Send real-time alerts to the system administrator for immediate action
- Record SSH session activity logs for improved security and audit compliance

Abaku
As na disku.

SSH – Bad Habits and Their Solutions

Thank You

mag. Sergej Rožman
ABAKUS plus d.o.o.
Ljubljanska c. 24a, Kranj, Slovenija

e-mail: sergej.rozman@abakus.si