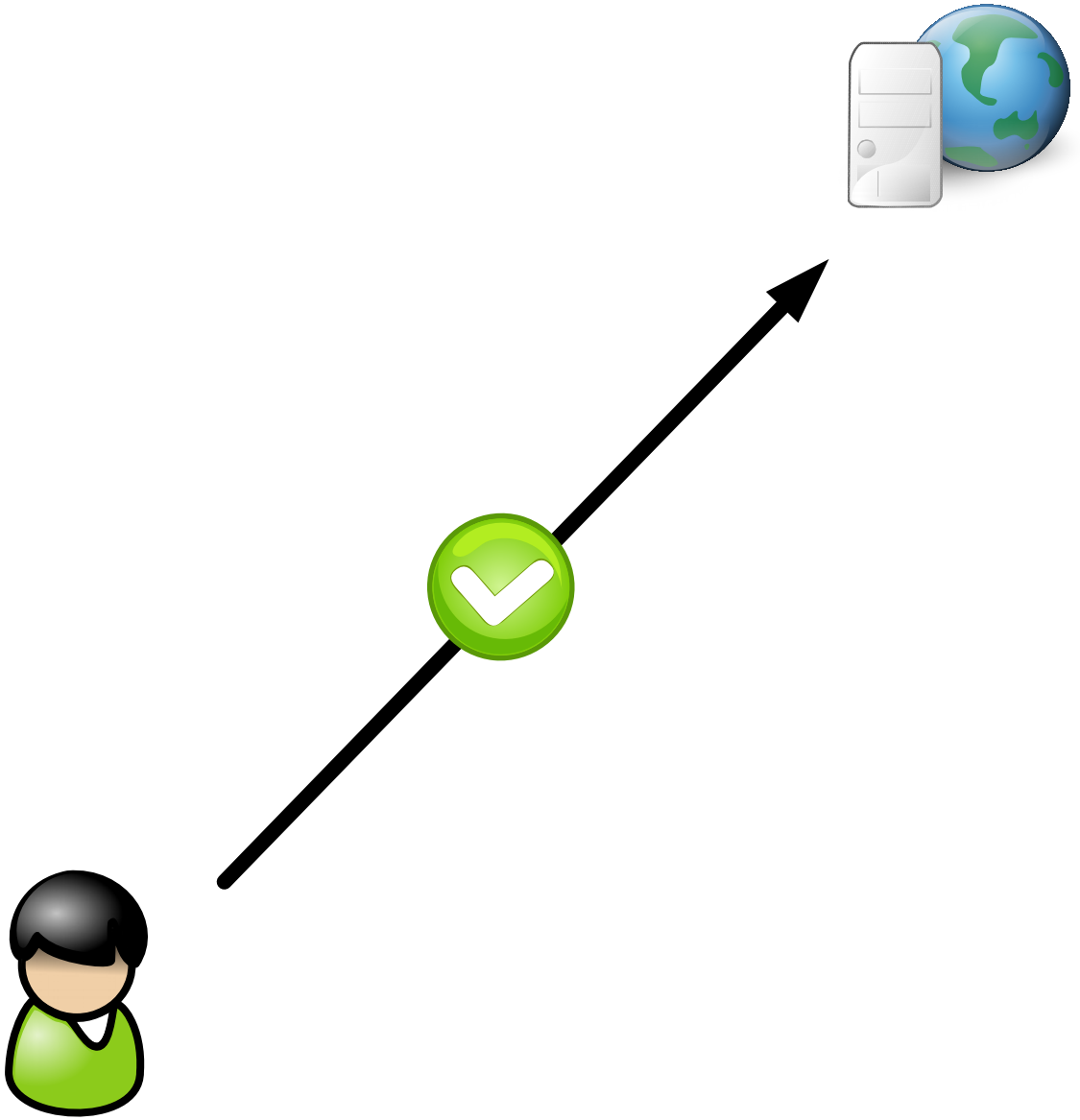
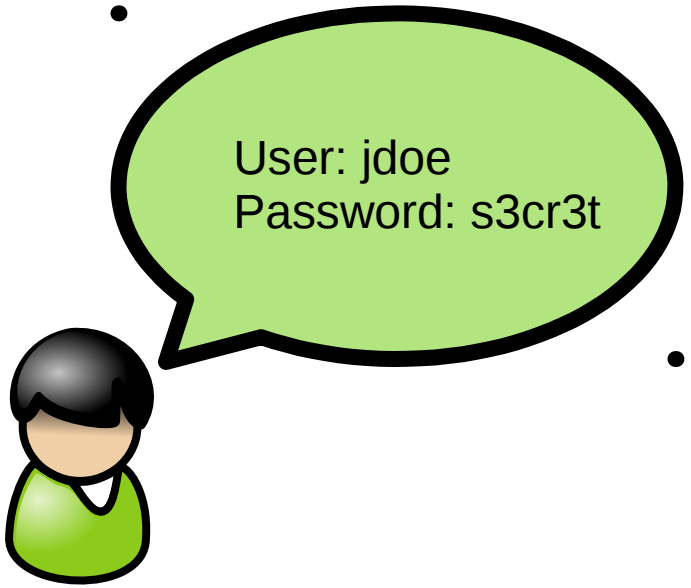
One Time Passwords

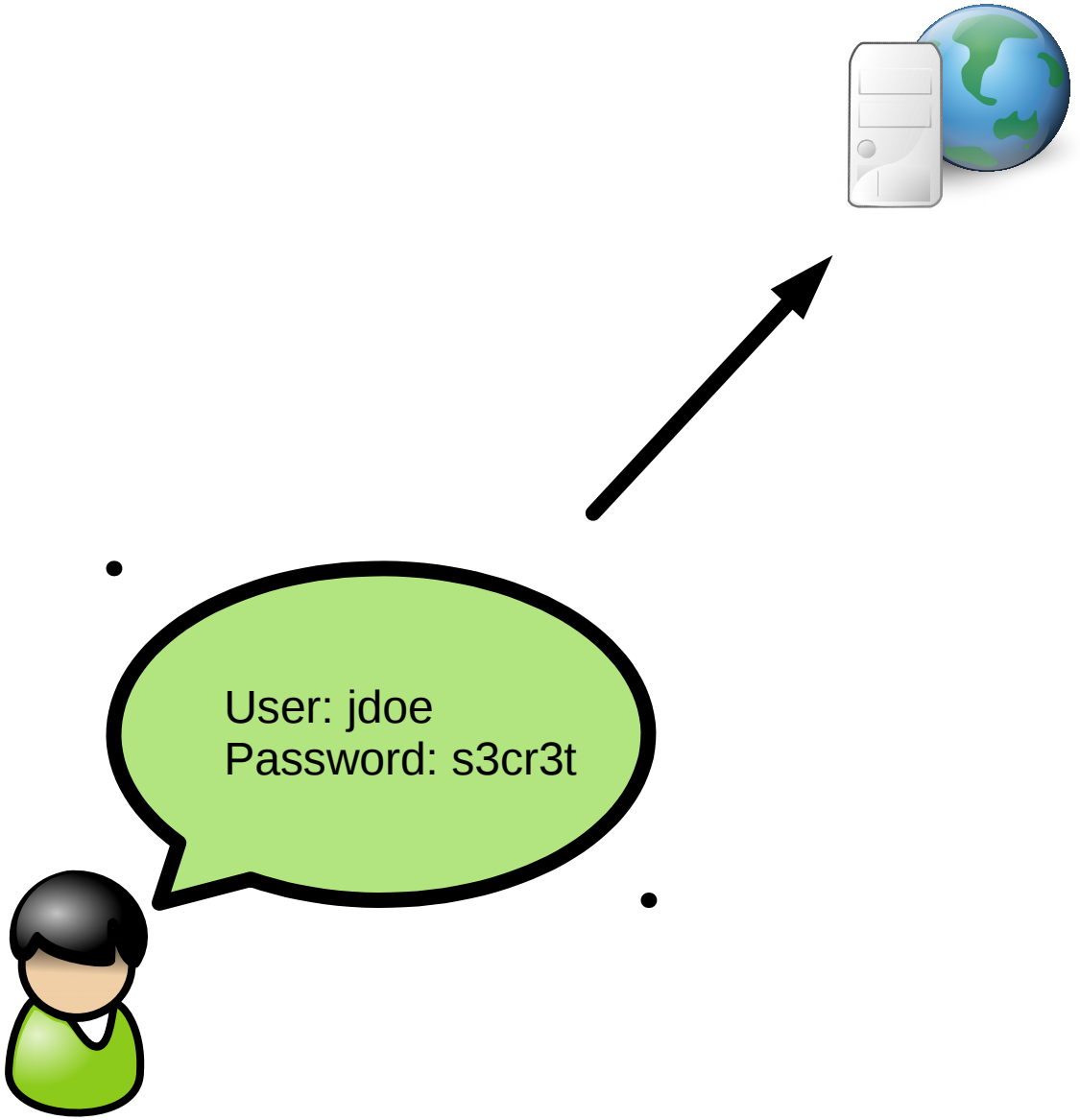
fhLUG, Hagenberg, 2016-03-08

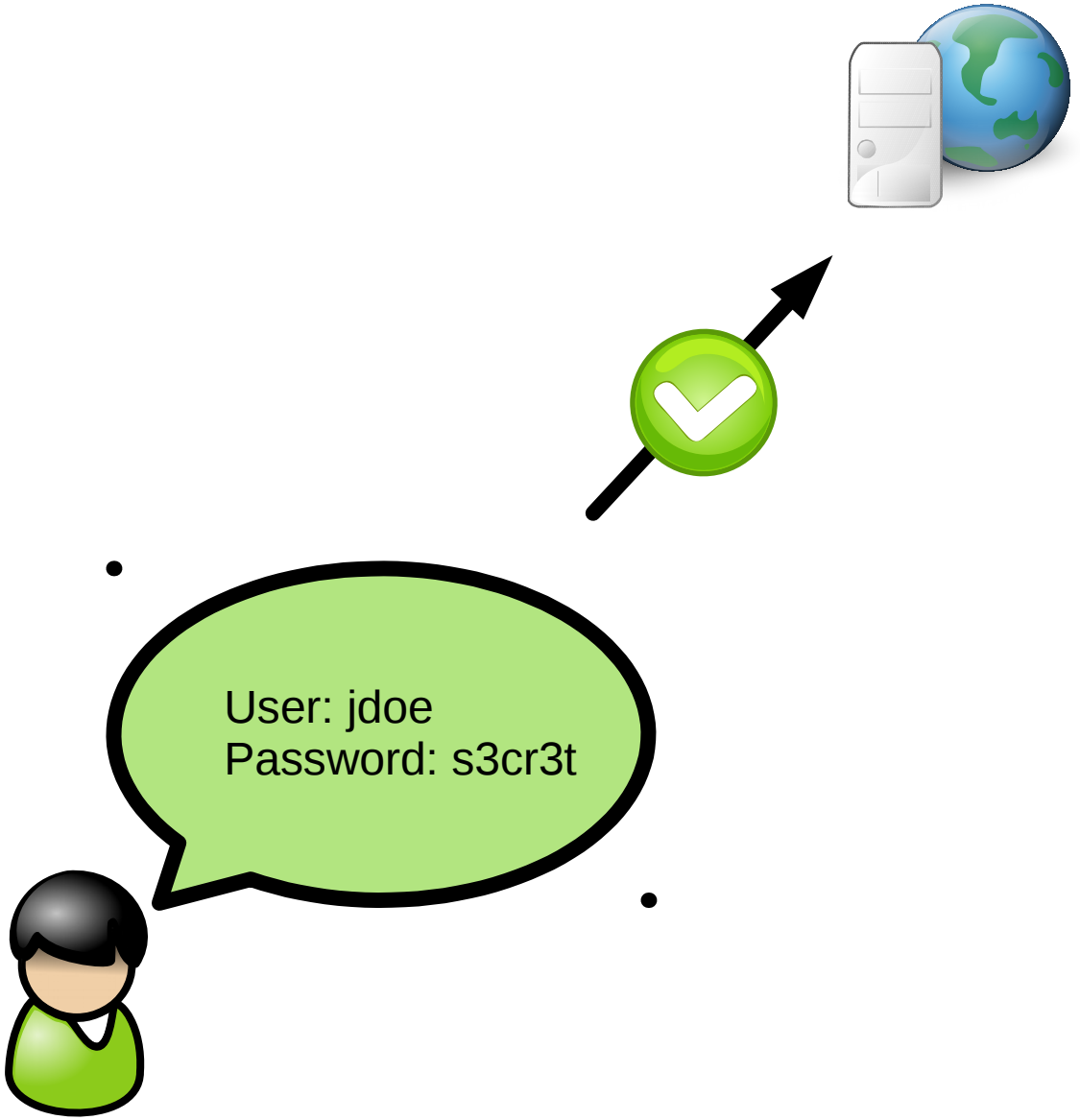
One Time Passwords

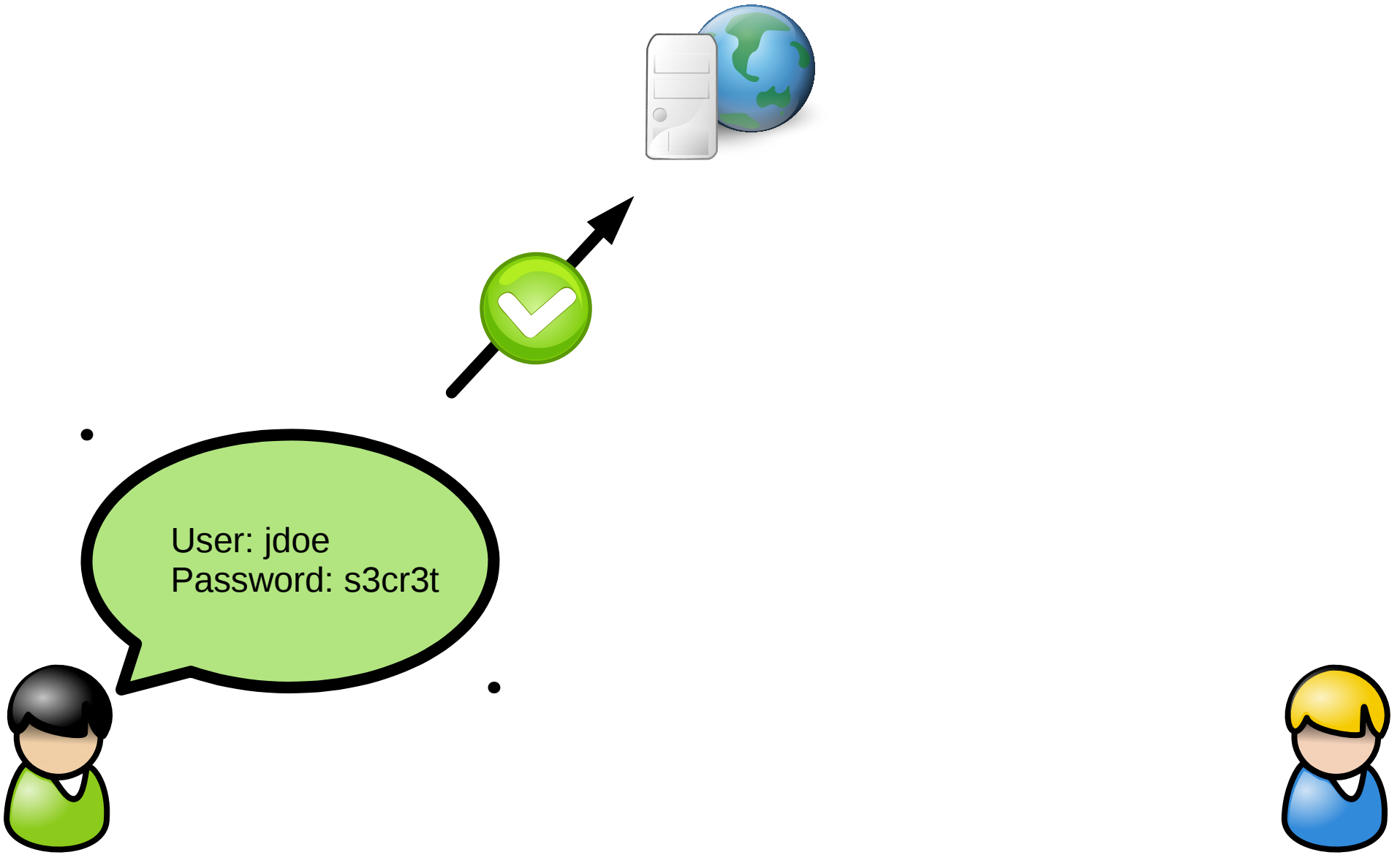
fhLUG, Hagenberg, 2016-03-08

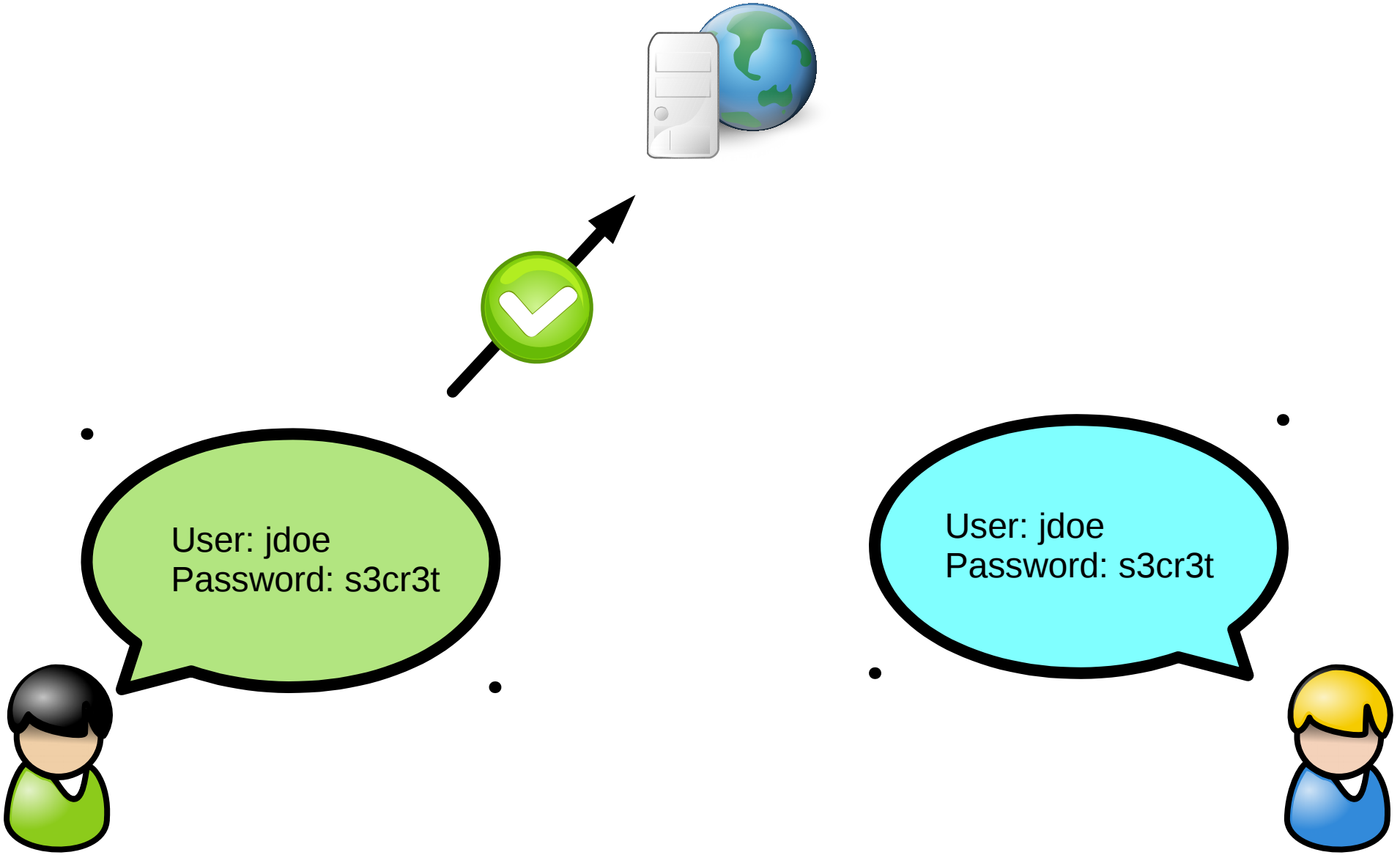


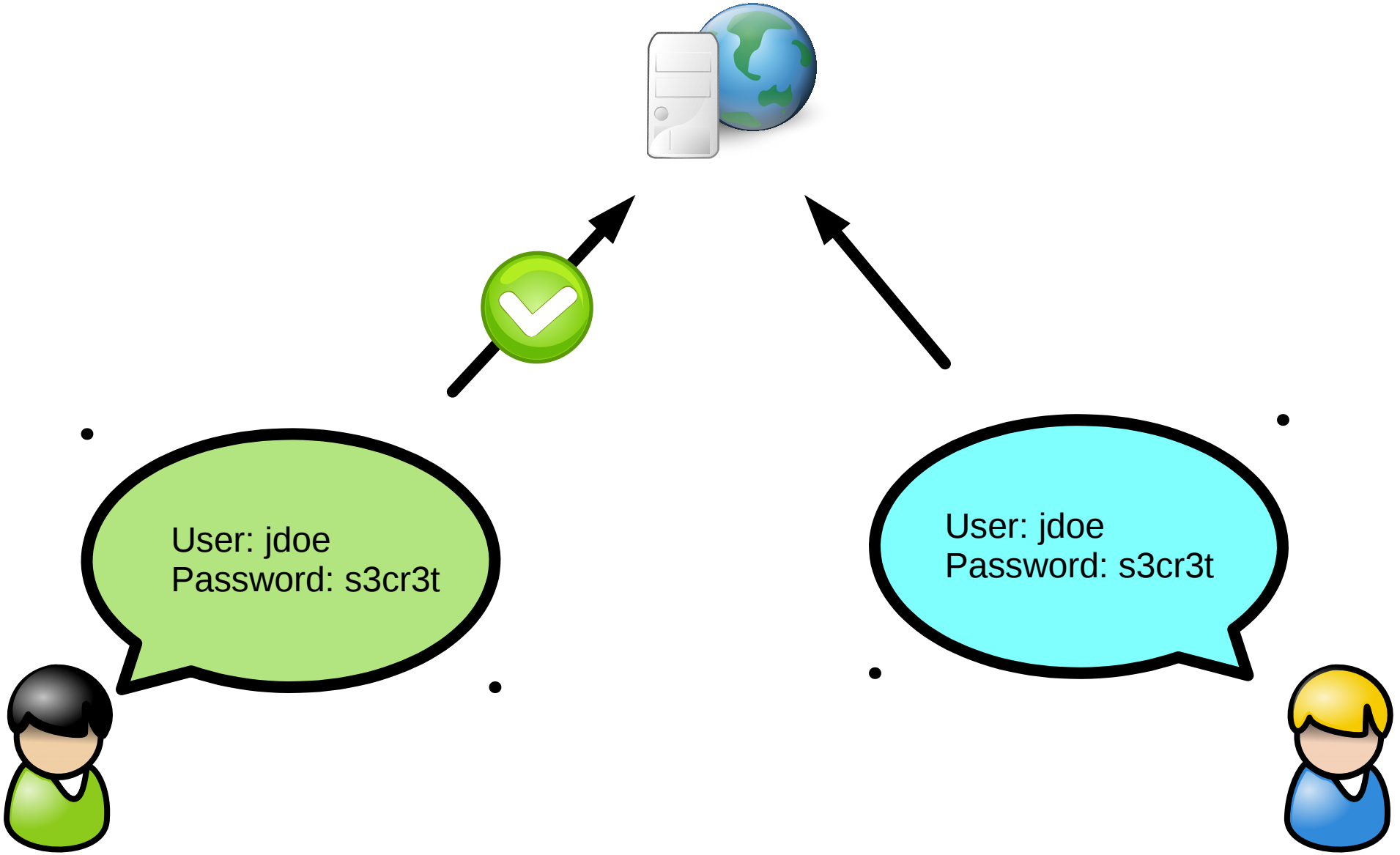

User: jdoe
Password: s3cr3t

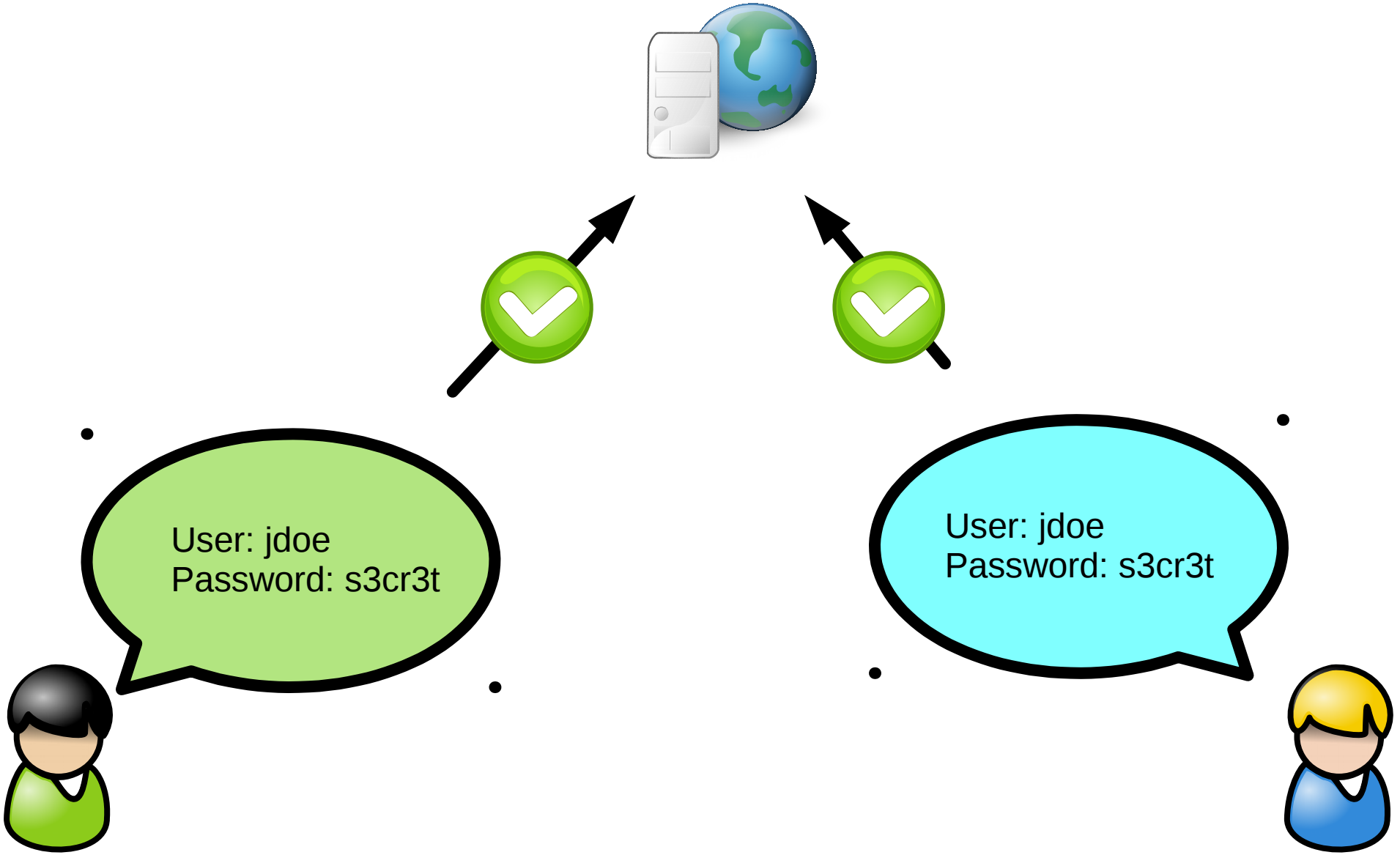

User: jdoe
Password: s3cr3t

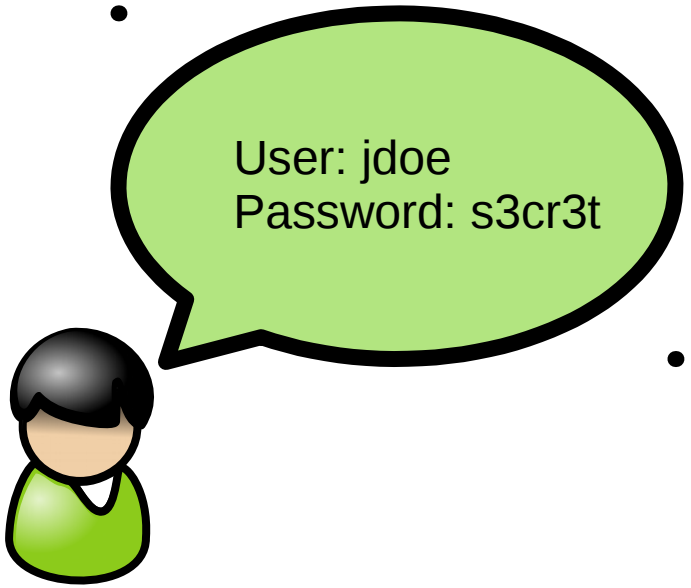

User: jdoe
Password: s3cr3t

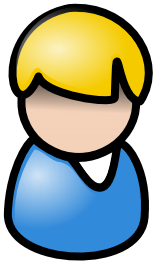

User: jdoe
Password: s3cr3t

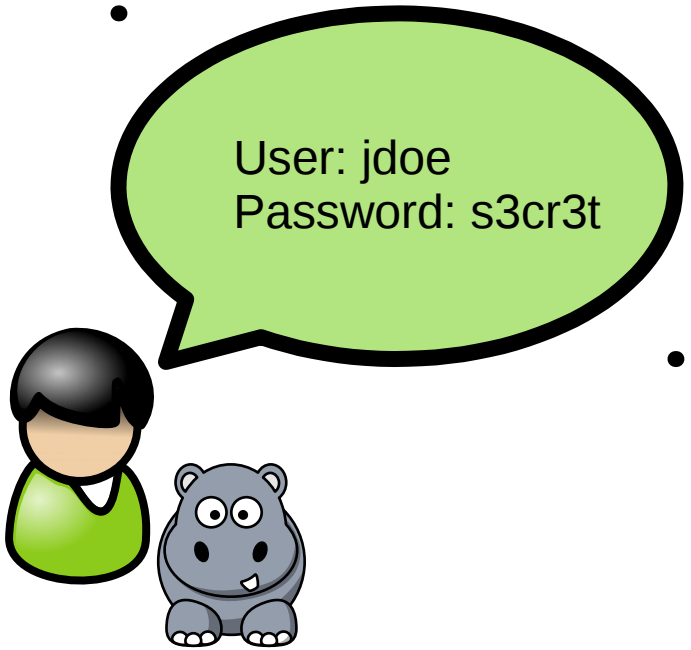

User: jdoe
Password: s3cr3t
User: jdoe
Password: s3cr3t

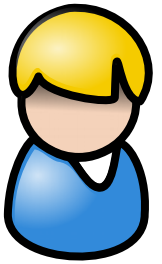

User: jdoe
Password: s3cr3t
User: jdoe
Password: s3cr3t

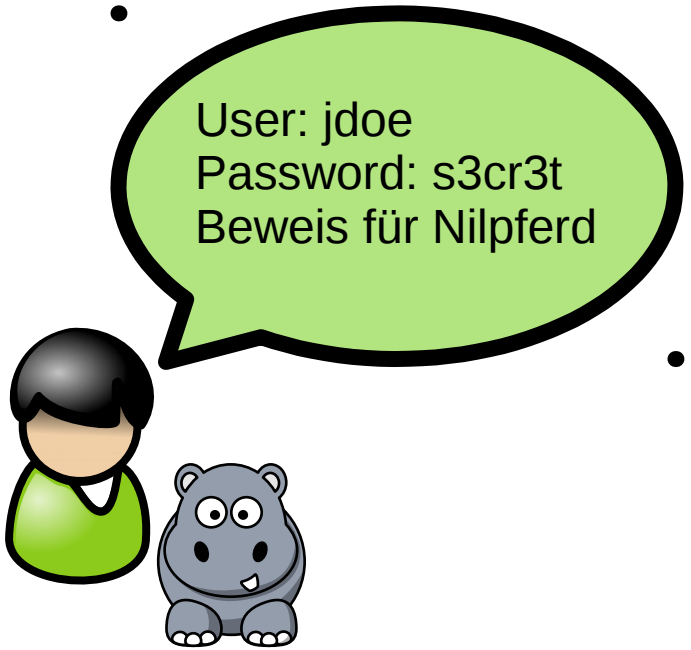

User: jdoe
Password: s3cr3t
User: jdoe
Password: s3cr3t

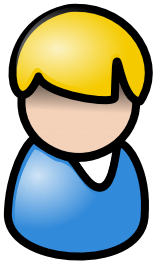

User: jdoe
Password: s3cr3t

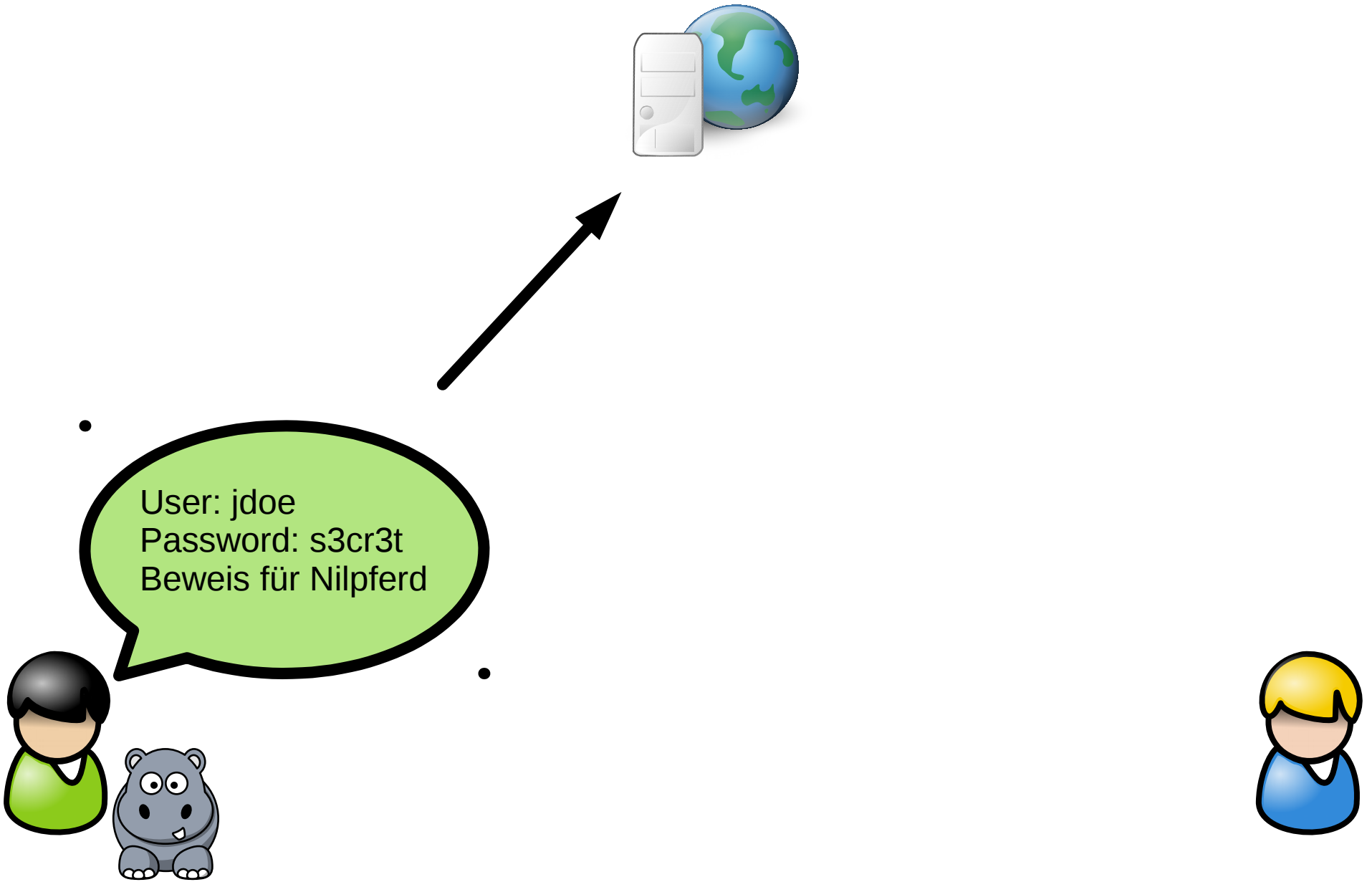


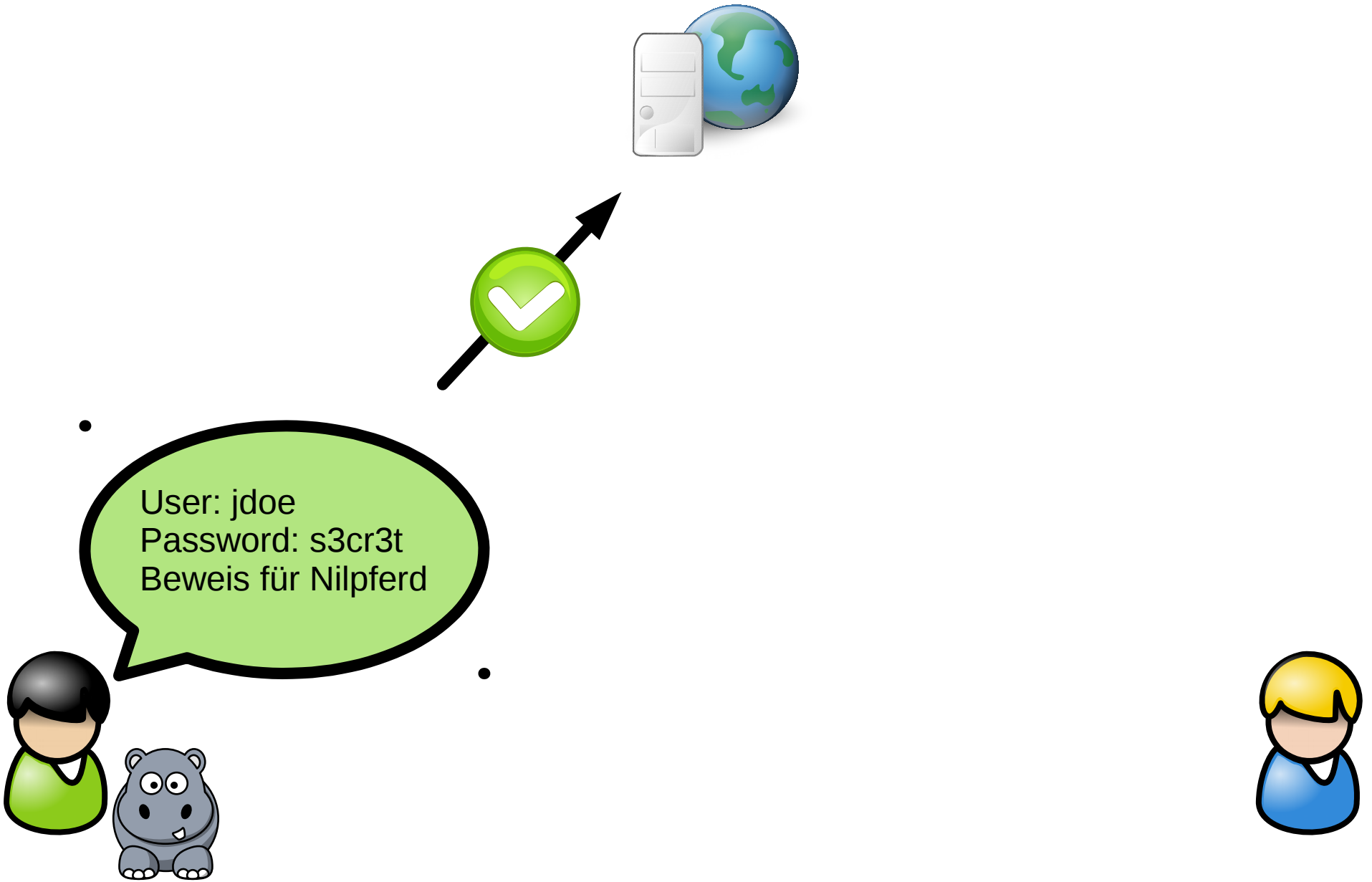

User: jdoe
Password: s3cr3t

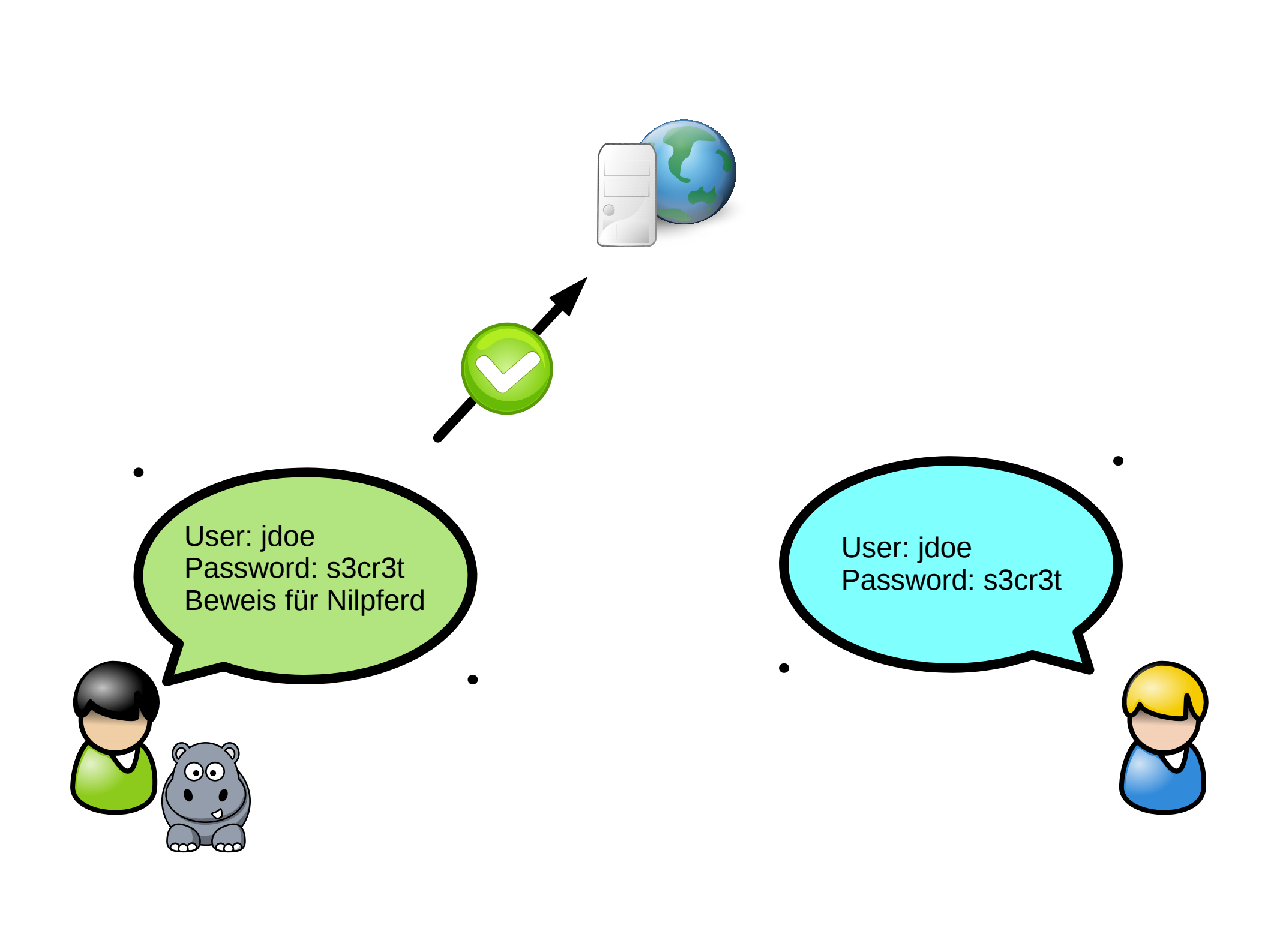


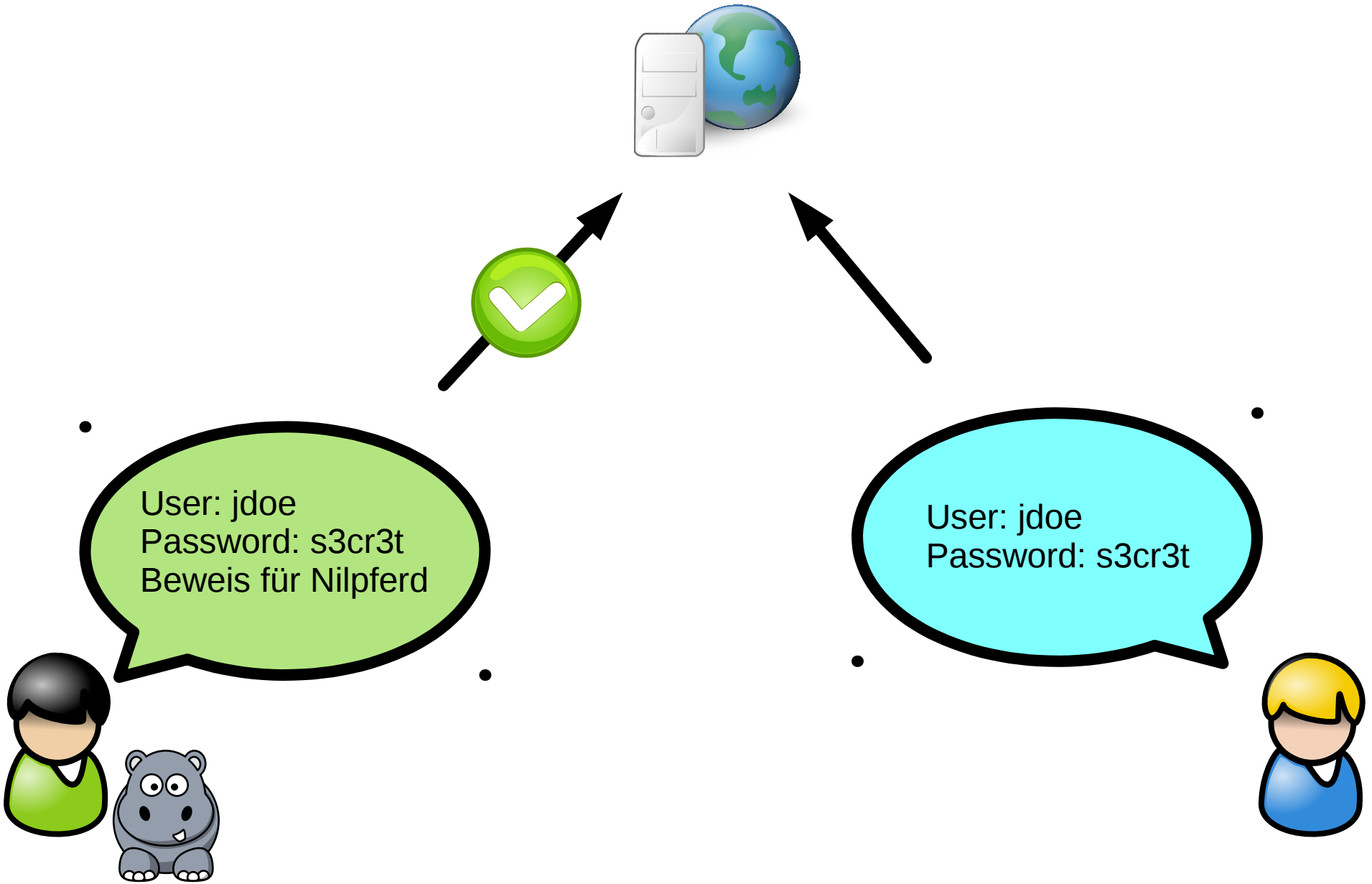

User: jdoe
Password: s3cr3t
Beweis für Nilpferd

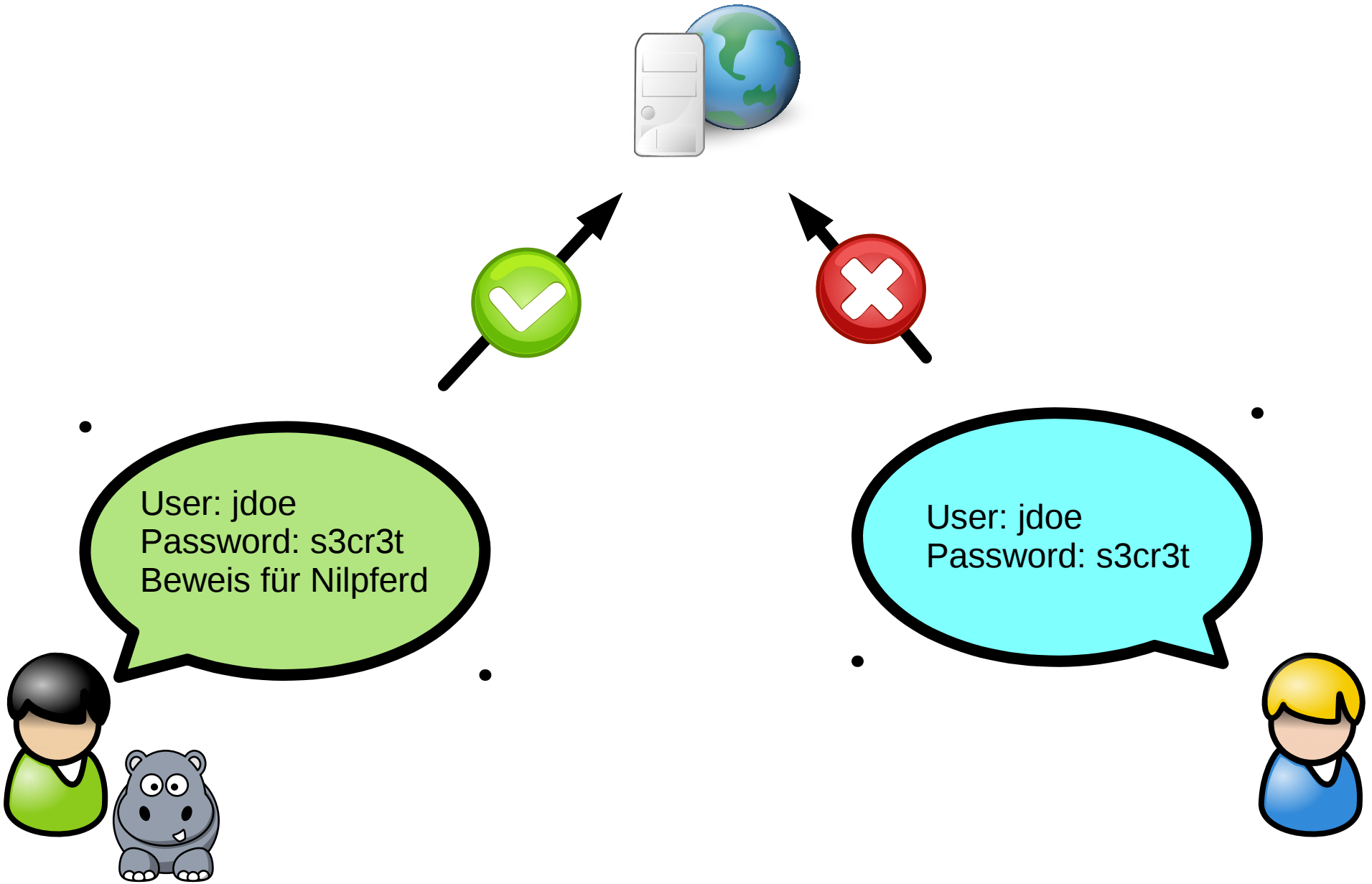


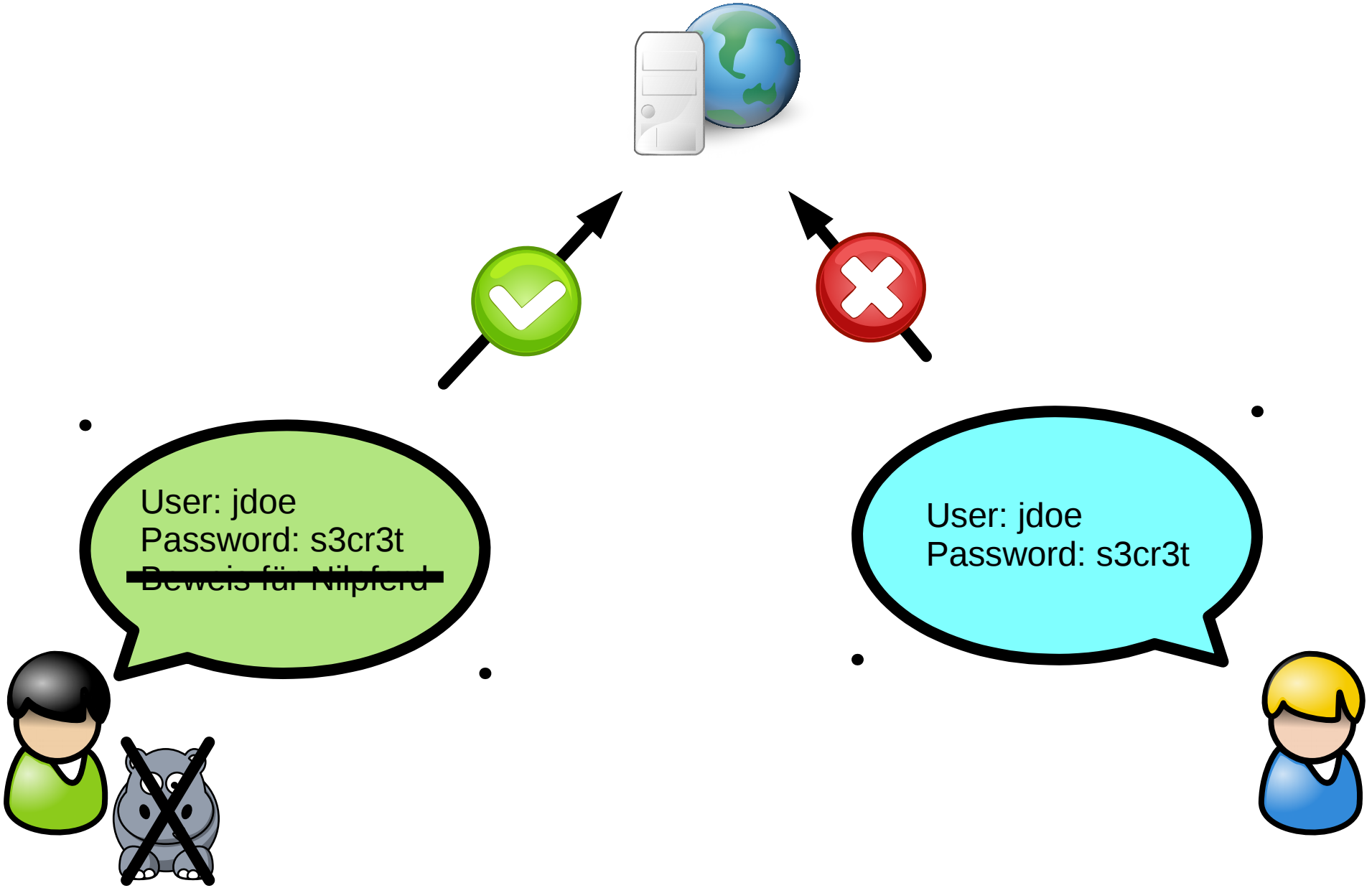

User: jdoe
Password: s3cr3t
Beweis für Nilpferd

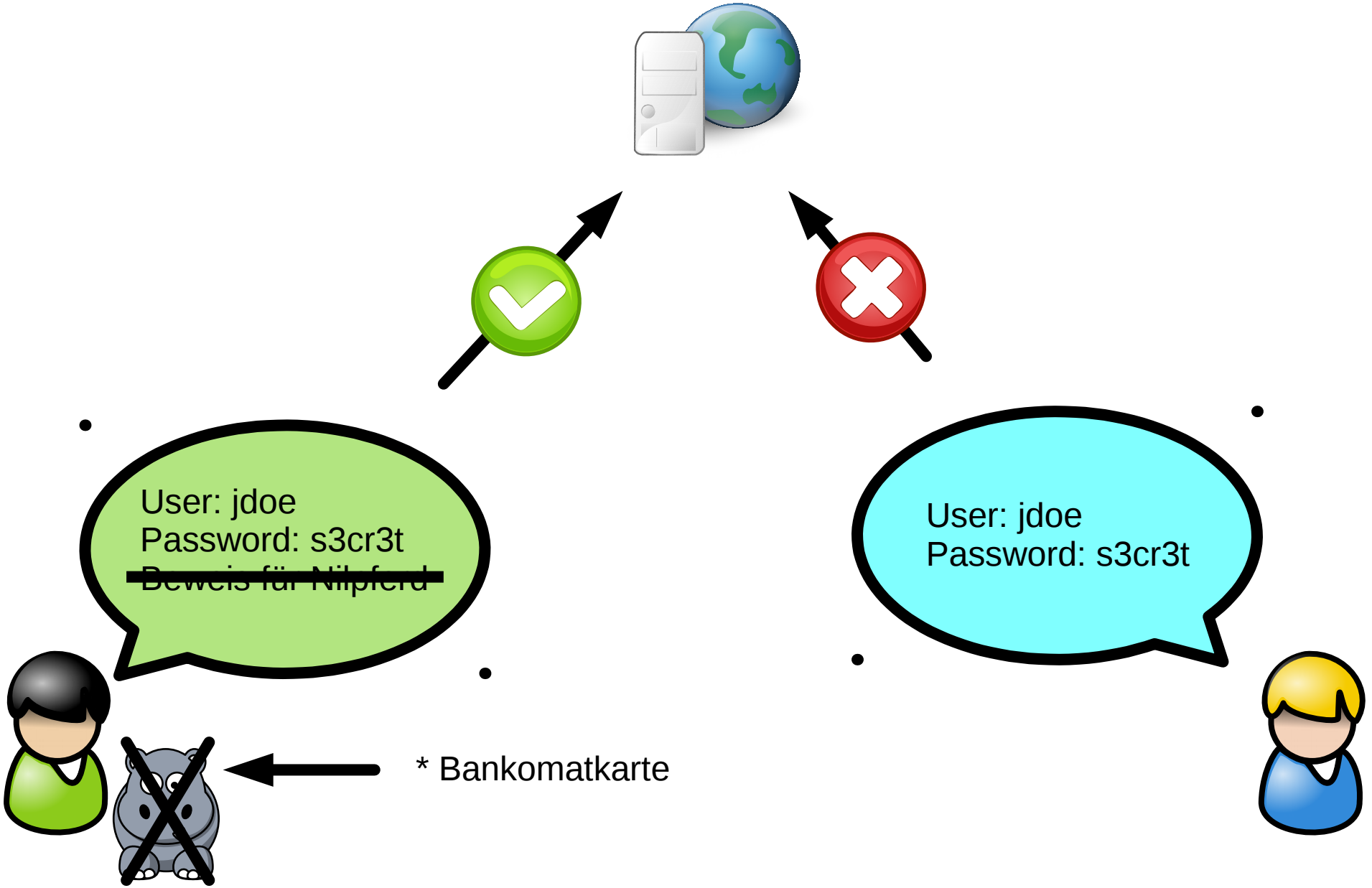

User: jdoe
Password: s3cr3t
Beweis für Nilpferd

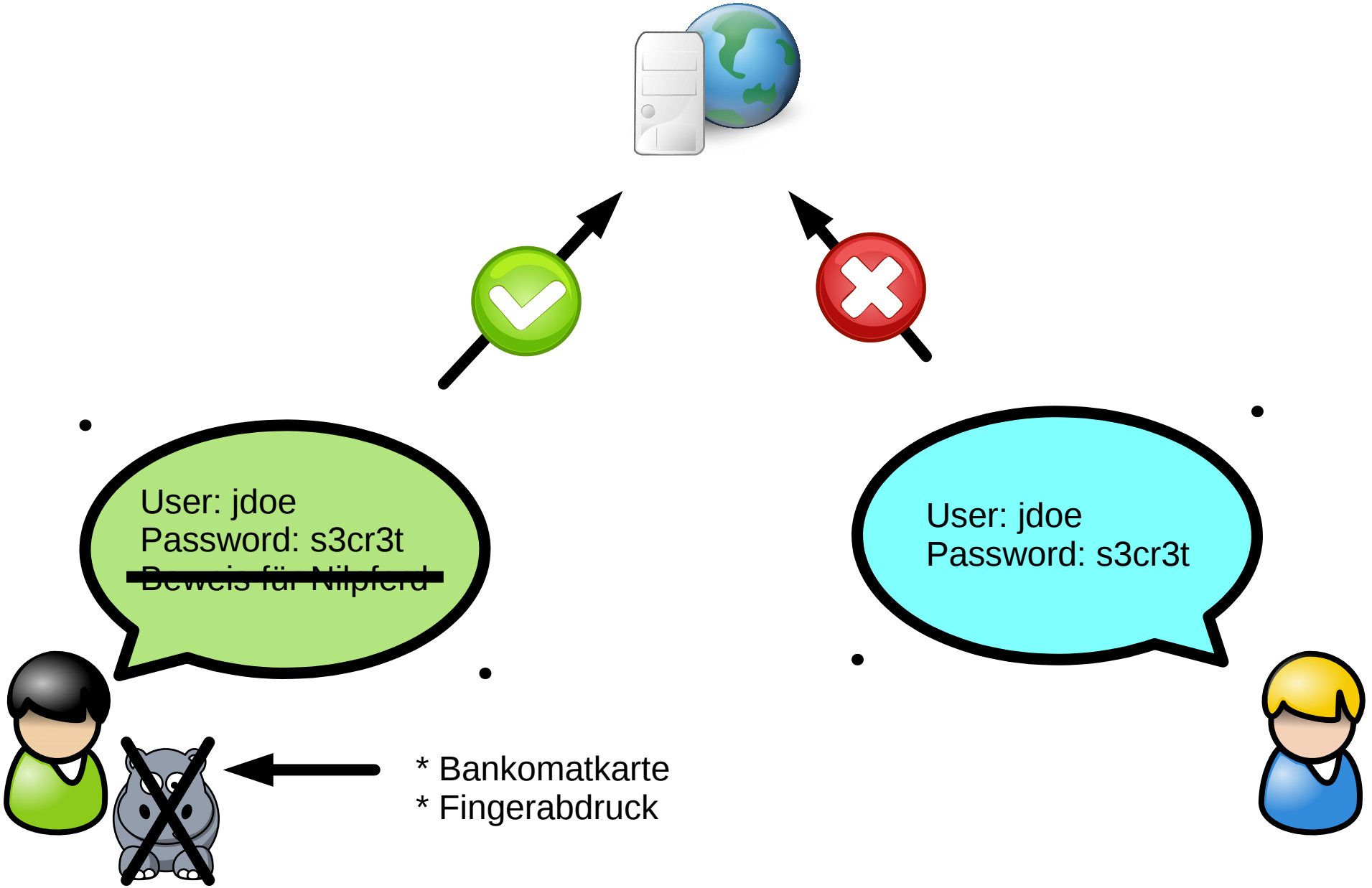

User: jdoe
Password: s3cr3t
Beweis für Nilpferd
User: jdoe
Password: s3cr3t

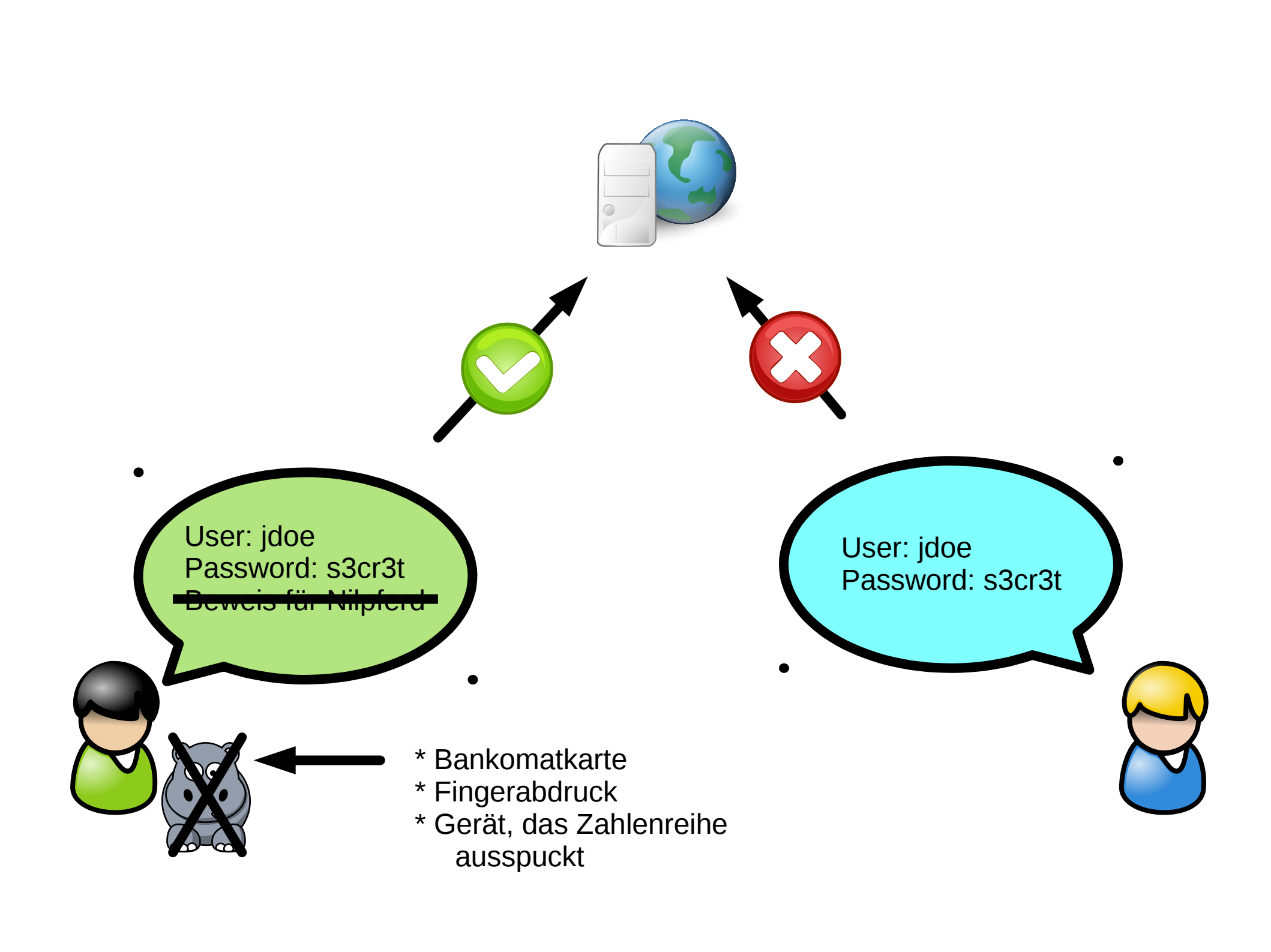

User: jdoe
Password: s3cr3t
Beweis für Nilpferd
User: jdoe
Password: s3cr3t


User: jdoe
Password: s3cr3t
Beweis für Nilpferd
User: jdoe
Password: s3cr3t


User: jdoe
Password: s3cr3t
~~Beweis für Nilpferd~~
User: jdoe
Password: s3cr3t


User: jdoe
Password: s3cr3t
~~Beweis für Nilpferd~~
User: jdoe
Password: s3cr3t
* Bankomatkarte


User: jdoe
Password: s3cr3t
~~Beweis für Nilpferd~~
User: jdoe
Password: s3cr3t
* Bankomatkarte
* Fingerabdruck


User: jdoe
Password: s3cr3t
~~Beweis für Nilpferd~~
User: jdoe
Password: s3cr3t
* Bankomatkarte
* Fingerabdruck
* Gerät, das Zahlenreihe
ausspuckt


OTP c200
672 736
ONE TIME PASSWORD


OTP c200
672 736
ONE TIME PASSWORD

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Accessibility Hilfe

Go...

https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

Suchen

Google Play

Search

Apps

Categories

Home

Top Charts

New Releases

My apps

Shop

Games

Family

Editors' Choice

My account

My Play activity

My wishlist

Redeem

Buy gift card

Parent Guide

Google Authenticator

Top Developer

Google Inc. Tools

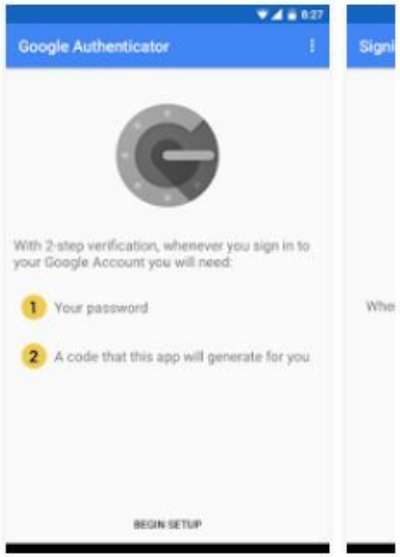
126,622

PEGI 3

You don't have any devices

Add to Wishlist

Install



Google Authenticator generates 2-step verification codes on your phone.

Set up Google Authenticator

Install the Google Authenticator app for Android.

1. On your phone, go to the Google Play Store.
2. Search for **Google Authenticator**.
   (Download from the Google Play Store)
3. Download and install the application.

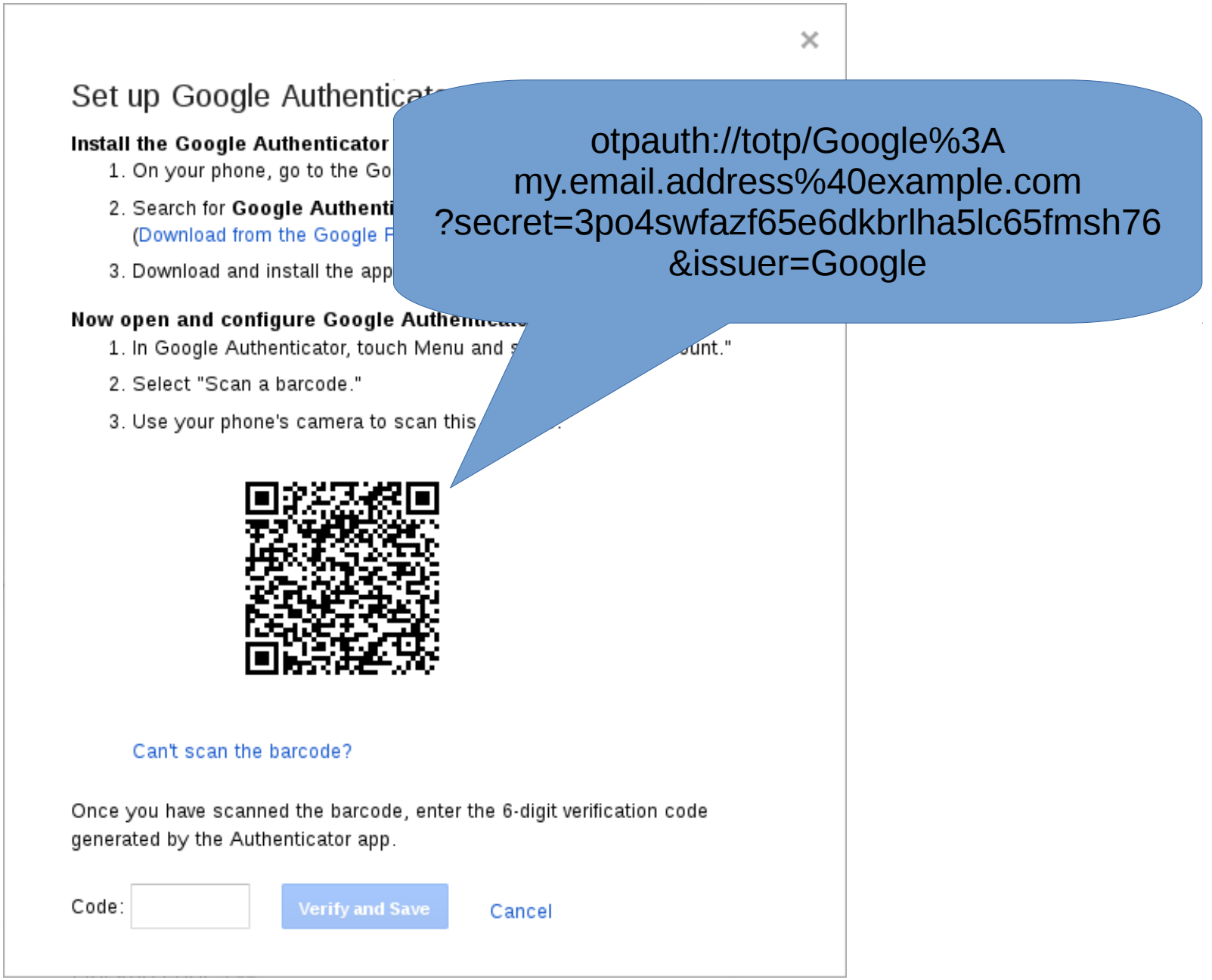
Now open and configure Google Authenticator.

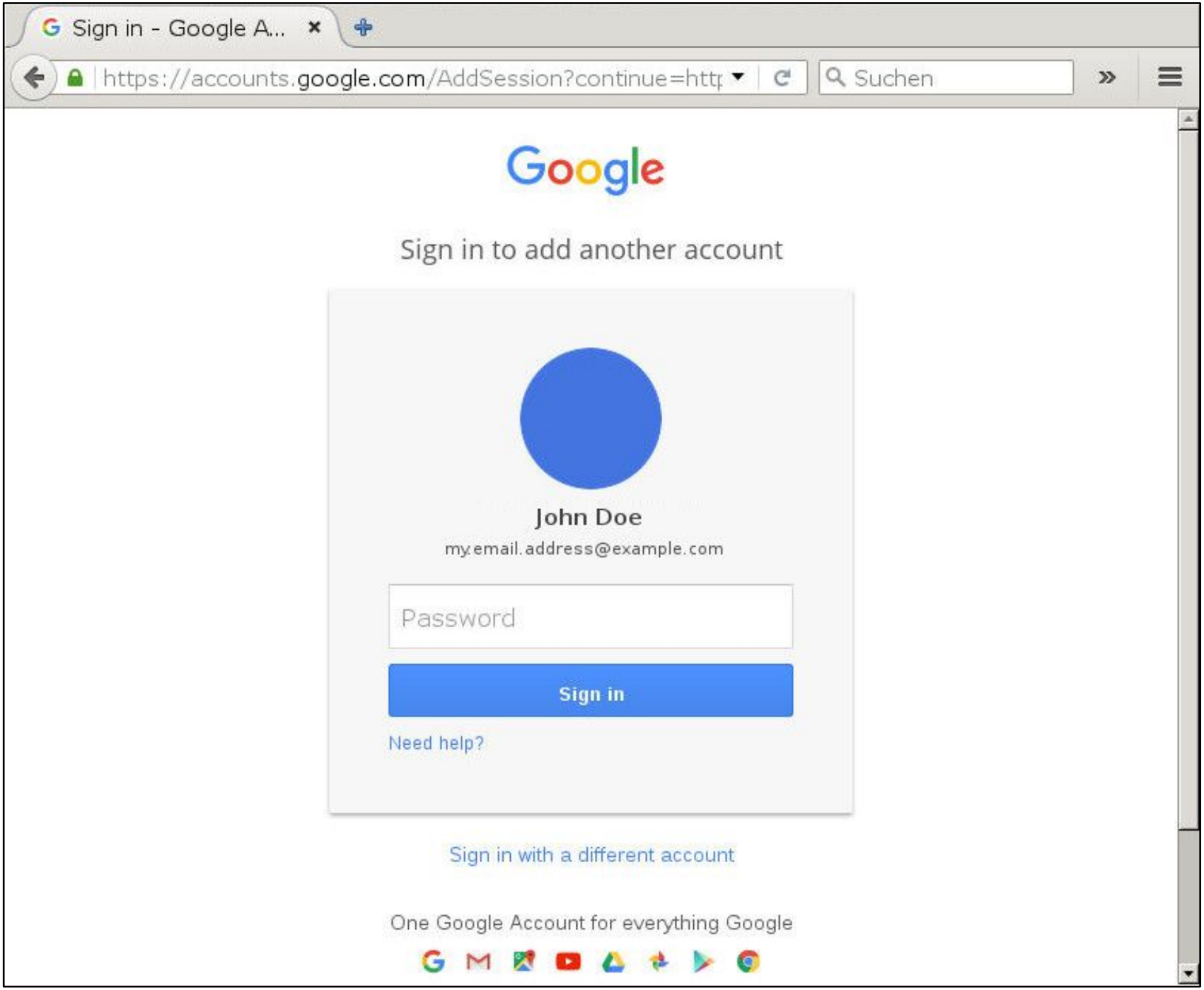
1. In Google Authenticator, touch Menu and select "Set up account."
2. Select "Scan a barcode."
3. Use your phone's camera to scan this barcode.

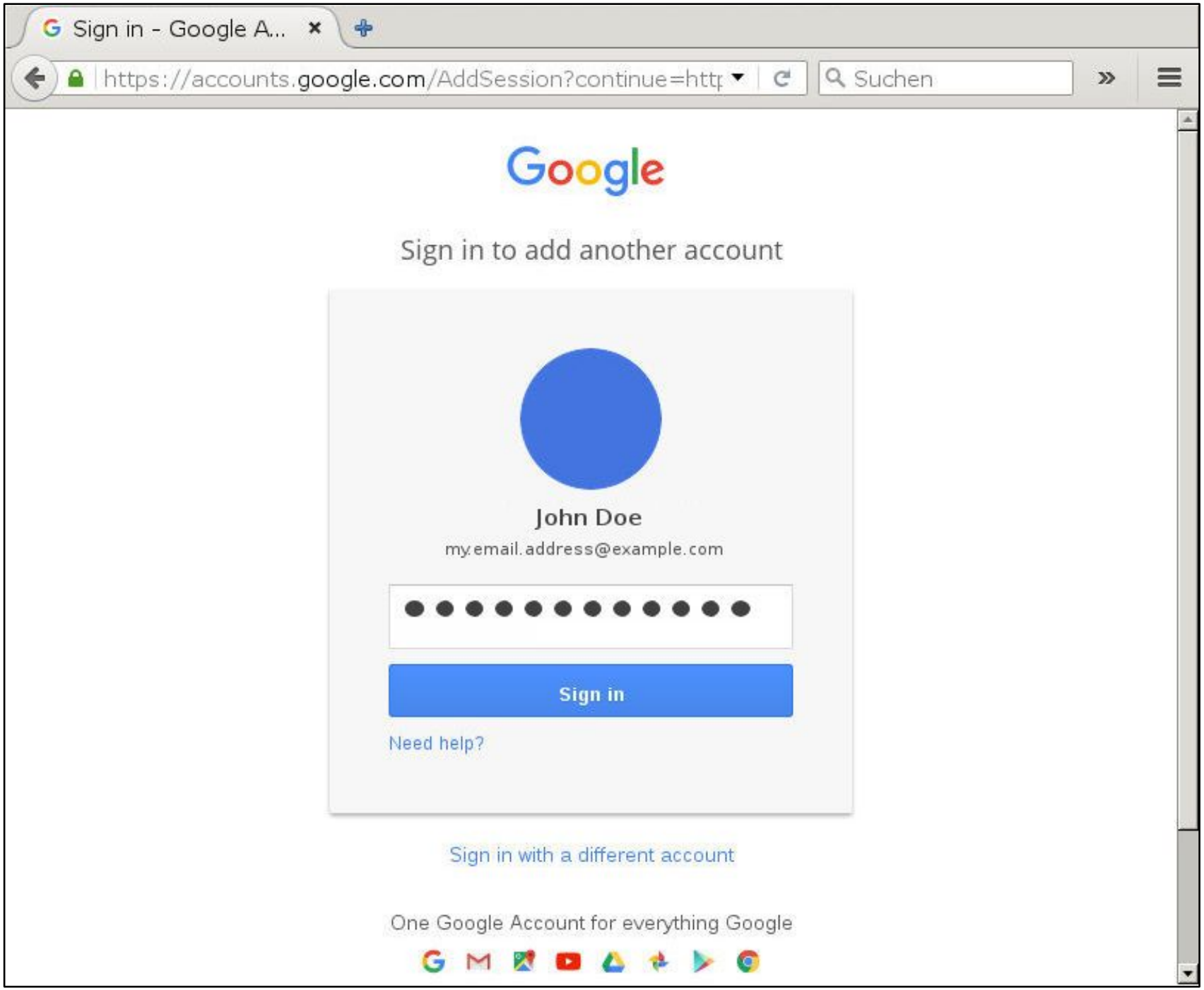
Can't scan the barcode?

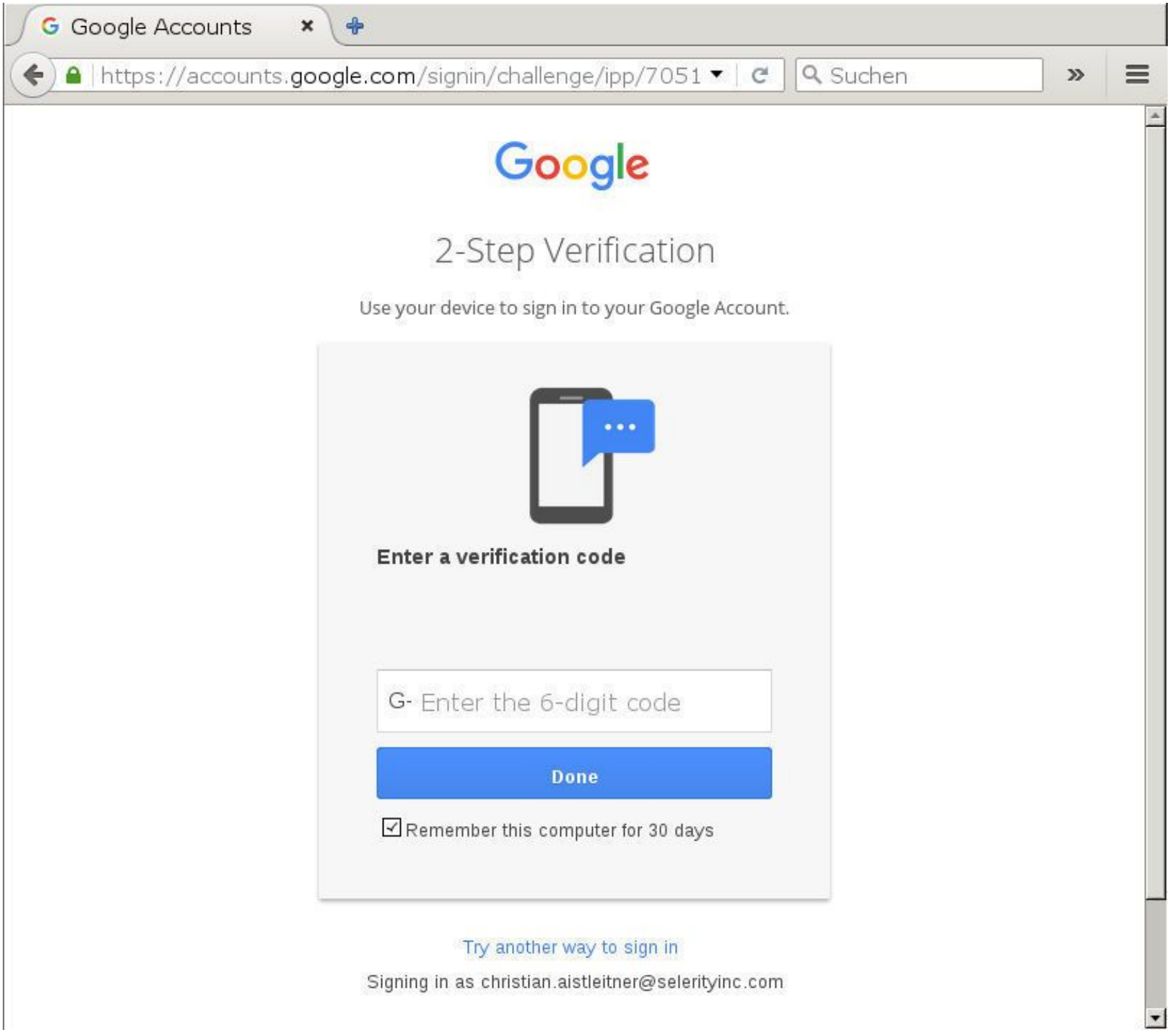
Once you have scanned the barcode, enter the 6-digit verification code generated by the Authenticator app.

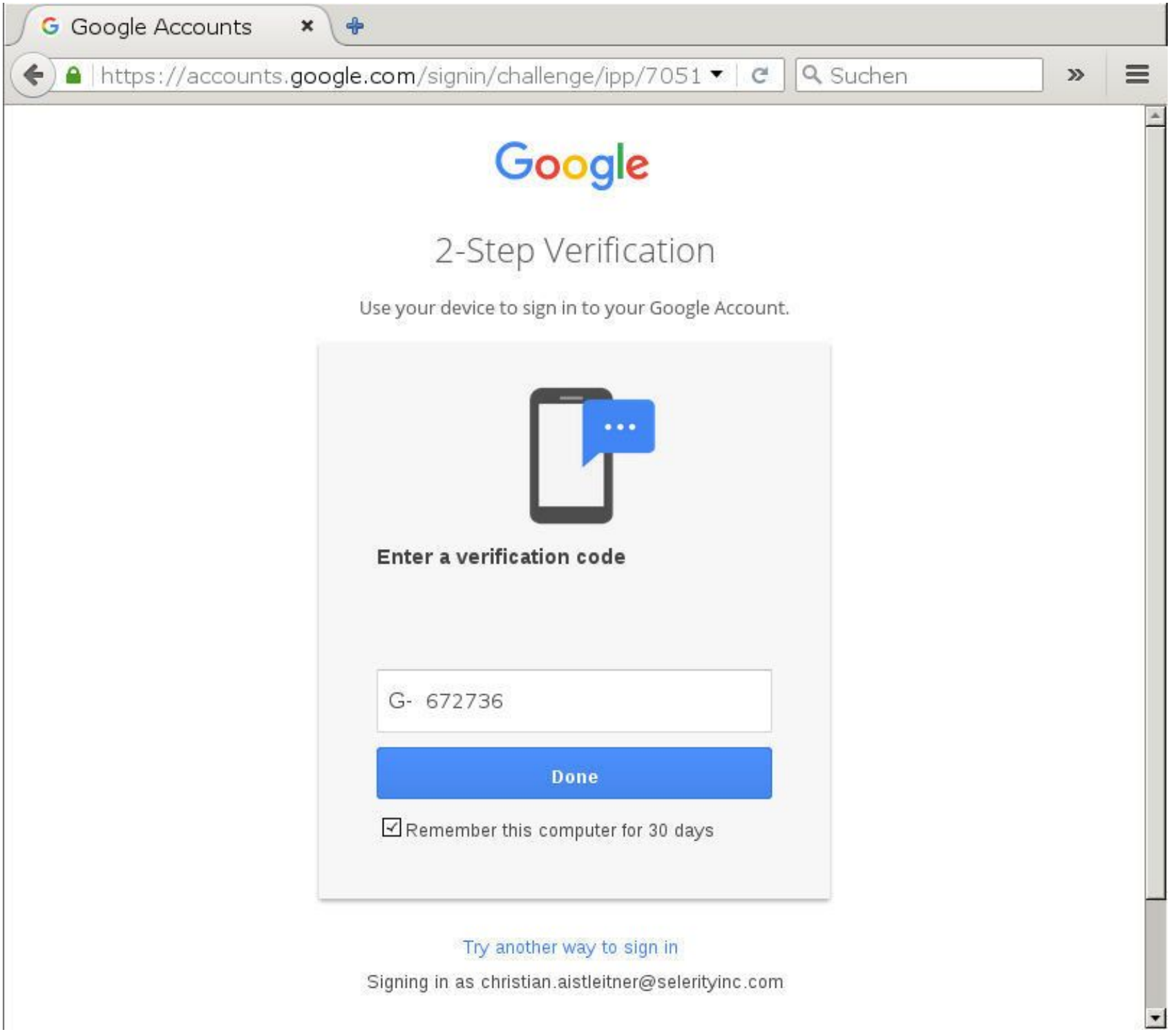
Code: Verify and Save Cancel

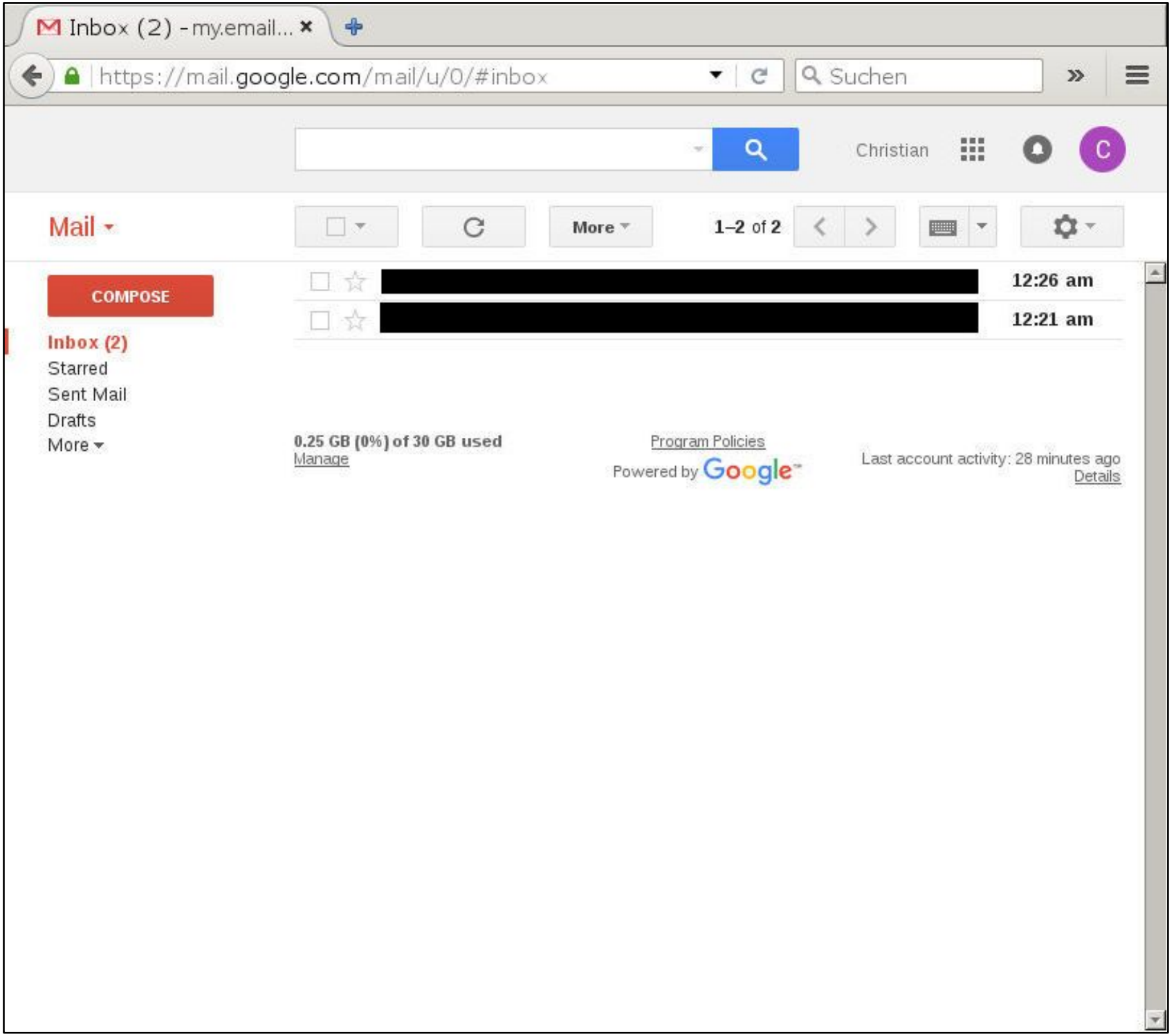

Set up Google Authenticat
Install the Google Authenticator
1. On your phone, go to the Go
2. Search for Google Authenti
(Download from the Google P
3. Download and install the app
Now open and configure Google Authenticat
1. In Google Authenticator, touch Menu and s
ount."
2. Select "Scan a barcode."
3. Use your phone's camera to scan this
otpauth://totp/Google%3A
my.email.address%40example.com
?secret=3po4swfazf65e6dkbrlha5lc65fmsh76
&issuer=Google
Can't scan the barcode?
Once you have scanned the barcode, enter the 6-digit verification code generated by the Authenticator app.
Code:
Verify and Save
Cancel


Sign in - Google A...
https://accounts.google.com/AddSession?continue=http
Suchen
Google
Sign in to add another account
John Doe
my.email.address@example.com
Password
Sign in
Need help?
Sign in with a different account
One Google Account for everything Google


Sign in - Google A...
https://accounts.google.com/AddSession?continue=htt
Suchen
Google
Sign in to add another account
John Doe
my.email.address@example.com
Sign in
Need help?
Sign in with a different account
One Google Account for everything Google


Google Accounts
https://accounts.google.com/signin/challenge/ipp/7051
Suchen
Google
2-Step Verification
Use your device to sign in to your Google Account.
Enter a verification code
G- Enter the 6-digit code
Done
Remember this computer for 30 days
Try another way to sign in
Signing in as christian.aistleitner@selerityinc.com


Google Accounts
https://accounts.google.com/signin/challenge/ipp/7051
Suchen
Google
2-Step Verification
Use your device to sign in to your Google Account.
Enter a verification code
G- 672736
Done
Remember this computer for 30 days
Try another way to sign in
Signing in as christian.aistleitner@selerityinc.com


Inbox (2) - my.email...
https://mail.google.com/mail/u/0/#inbox
Suchen
Christian
C
Mail
More
1–2 of 2
COMPOSE
[redacted]
12:26 am
[redacted]
12:21 am
Inbox (2)
Starred
Sent Mail
Drafts
More
0.25 GB (0%) of 30 GB used
Manage
Program Policies
Powered by Google
Last account activity: 28 minutes ago
Details

Prominent Open OTP Variants

- S/KEY
  - 1995, MD4 (MD5, SHA1)
  - RFC 1760, RFC 1938, RFC 2289
- mOTP
  - 2003, MD5
  - motp.sourceforge.net
- OATH HOTP
  - 2005, HMAC SHA1, Counter based
  - RFC 4226
- OATH TOTP
  - 2011, HMAC SHA1 (SHA256), Time based
  - RFC 6238

Prominent Open OTP Variants

- S/KEY
  - 1995, MD4 (MD5, SHA1)
  - RFC 1760, RFC 1938, RFC 2289
- mOTP
  - 2003, MD5
  - motp.sourceforge.net
- OATH HOTP
  - 2005, HMAC SHA1, Counter based
  - RFC 4226
- OATH TOTP
  - 2011, HMAC SHA1 (SHA256), Time based
  - RFC 6238

Prominent Open OTP Variants

- S/KEY
  - 1995, MD4 (MD5, SHA1)
  - RFC 1760, RFC 1938, RFC 2289
- mOTP
  - 2003, MD5
  - motp.sourceforge.net
- OATH HOTP
  - 2005, HMAC SHA1, Counter based
  - RFC 4226
- OATH TOTP
  - 2011, HMAC SHA1 (SHA256), Time based
  - RFC 6238

Prominent Open OTP Variants

- S/KEY
  - 1995, MD4 (MD5, SHA1)
  - RFC 1760, RFC 1938, RFC 2289
- mOTP
  - 2003, MD5
  - motp.sourceforge.net
- OATH HOTP
  - 2005, HMAC SHA1, Counter based
  - RFC 4226
- OATH TOTP
  - 2011, HMAC SHA1 (SHA256), Time based
  - RFC 6238

Prominent Open OTP Variants

- S/KEY
  - 1995, MD4 (MD5, SHA1)
  - RFC 1760, RFC 1938, RFC 2289
- mOTP
  - 2003, MD5
  - motp.sourceforge.net
- OATH HOTP
  - 2005, HMAC SHA1, Counter based
  - RFC 4226
- OATH TOTP
  - 2011, HMAC SHA1 (SHA256), Time based
  - RFC 6238

OATH HOTP

Generate Key

Counter = 0

OATH-HOTP(Key, Counter):

HS = HMAC-SHA1(Key, Counter)

Offset = Lowest 4 bits of HS

OTP = (lower 31 bits of HS[Offset:4]) mod 1000000

Counter = Counter + 1

HMAC-SHA1

RFC 2104

HMAC-SHA1(Key, Counter):

ipad = 0x36363636...

opad = 0x5C5C5C5C...

SHA1((Key $\oplus$ opad) || SHA1((Key $\oplus$ ipad) || Counter))

OATH HOTP

Generate Key

Counter = 0

OATH-HOTP(Key, Counter):

HS = HMAC-SHA1(Key, Counter)

Offset = Lowest 4 bits of HS

OTP = (lower 31 bits of HS[Offset:4]) mod 1000000

Counter = Counter + 1

OATH HOTP

Generate Key

Counter = 0

OATH-HOTP(Key, Counter):

HS = HMAC-SHA1(Key, Counter)

Offset = Lowest 4 bits of HS

OTP = (lower 31 bits of HS[Offset:4]) mod 1000000

Counter = Counter + 1

OATH TOTP

Generate Key

OATH-TOTP(Key):

TS = Timestamp / 30

OTP = OATH-HOTP(Key, TS)

OATH TOTP

Generate Key

OATH-TOTP(Key):

TS = Timestamp / 30

OTP = OATH-HOTP(Key, TS)


OTP c200
672 736
ONE TIME PASSWORD

(c) Gemalto

(c) Gemalto

(c) Gemalto

(c) Gemalto

Server-Side

- Modules
  - PAM
  - OpenVPN
  - FreeRadius
  - Apache
  - ...
- Authentication Servers
  - PrivacyIDEA
  - LinOTP
  - YubiCloud OTP (can be self hosted)
  - ...

Round-up

- Hilft gegen Keylogging
- Hilft gegen Phishing
- Hilft gegen Shoulder-Surfing
- Hilft gegen neugieriges Netzwerk (Kein Replay)
  - Keine eigene Verschlüsselung
- Wenn jemand Password + OTP erraten hat, kommt er kein 2. mal rein.

- Server braucht Schlüssel im Klartext
  - Hilft nicht bei Servereinbruch
- Bei TOTP: Geräte brauchen Zeitsynchronisation
- Usability
- Authentifiziering der Person vs. Transaktion

Demo

- Ein OATH HOTP/TOPT Programm installieren
  - Computer: sudo apt-get oathtool
  - Smartphone: Google Authenticator

- http://otp.quelltextlich.at/

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Accessibility Hilfe

OTP Demo Page

otp.quelltextlich.at

Suchen

OTP Demo Page

Links

- Go to public page
- Go to protected page

Environment

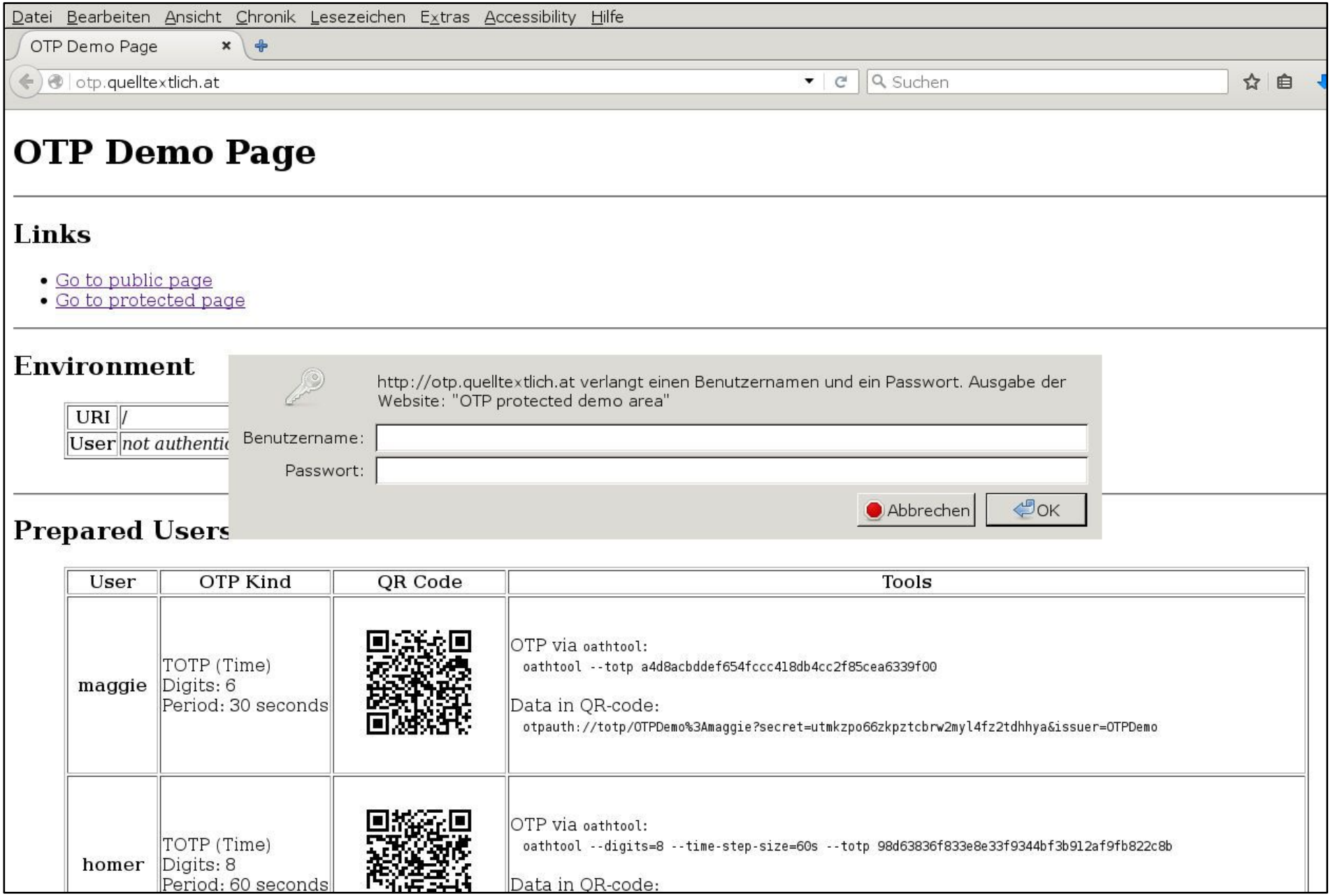
URI	/
User	*not authenticated*

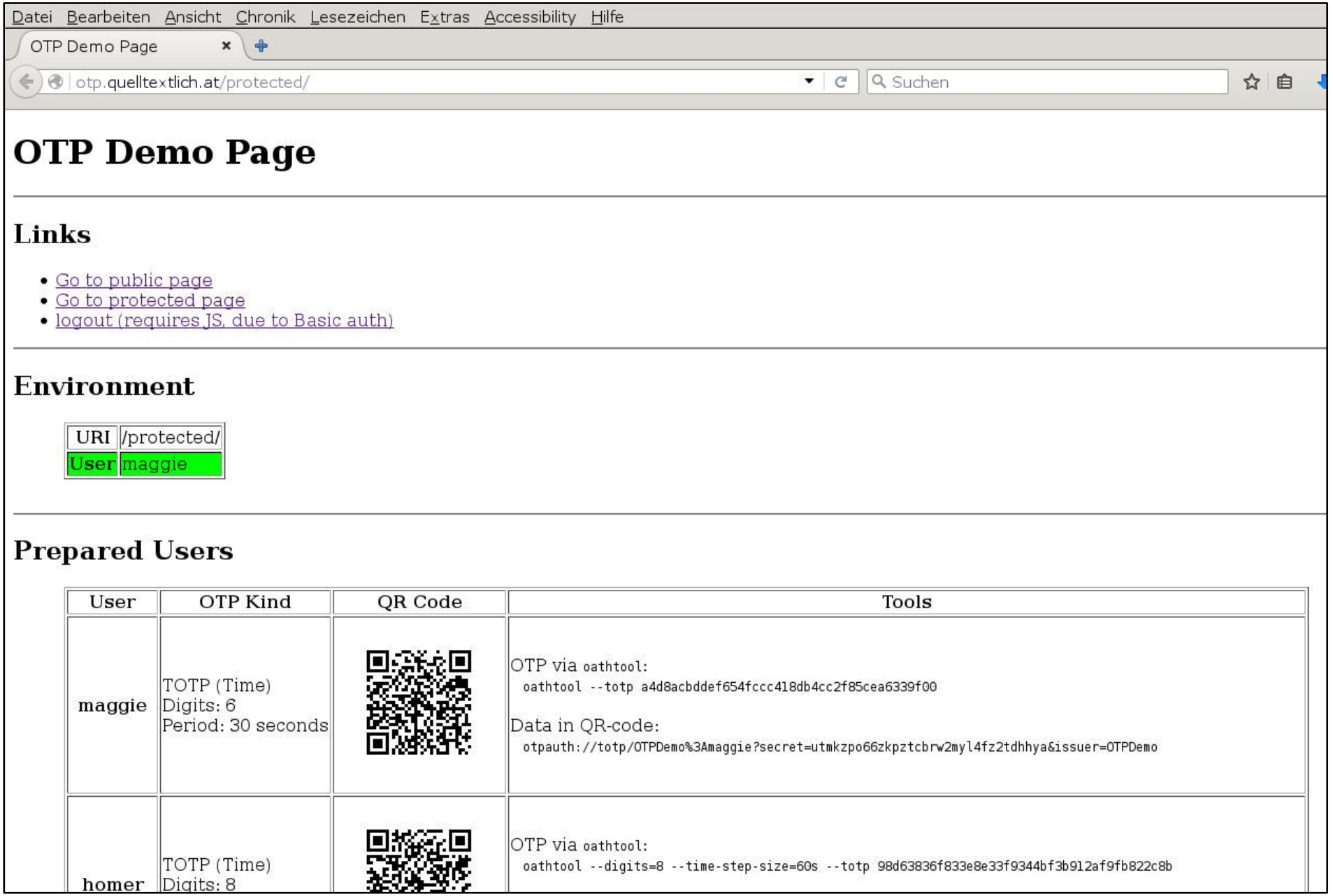
Prepared Users

User	OTP Kind	QR Code	Tools

maggie	TOTP (Time)
	Digits: 6
	Period: 30 seconds
			OTP via `oathtool`:
			`oathtool --totp a4d8acbddef654fccc418db4cc2f85cea6339f00`
			
			Data in QR-code:
			`otpauth://totp/OTPDemo%3Amaggie?secret=utmkzpo66zkpztcbrw2myl4fz2tdhhya&issuer=OTPDemo`

homer	TOTP (Time) Digits: 8 Period: 60 seconds		OTP via `oathtool`: `oathtool --digits=8 --time-step-size=60s --totp 98d63836f833e8e33f9344bf3b912af9fb822c8b` Data in QR-code:


Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Accessibility Hilfe
OTP Demo Page
otp.quelltextlich.at
Suchen
OTP Demo Page
Links
Go to public page
Go to protected page
Environment
URI /
User not authentic
http://otp.quelltextlich.at verlangt einen Benutzernamen und ein Passwort. Ausgabe der Website: "OTP protected demo area"
Benutzername:
Passwort:
Abbrechen
OK
Prepared Users
User
OTP Kind
QR Code
Tools
maggie
TOTP (Time)
Digits: 6
Period: 30 seconds
OTP via oathtool:
oathtool --totp a4d8acbddef654fccc418db4cc2f85cea6339f00
Data in QR-code:
otpauth://totp/OTPDemo%3Amaggie?secret=utmkzpo66zkpztcbrw2myl4fz2tdhhya&issuer=OTPDemo
homer
TOTP (Time)
Digits: 8
Period: 60 seconds
OTP via oathtool:
oathtool --digits=8 --time-step-size=60s --totp 98d63836f833e8e33f9344bf3b912af9fb822c8b
Data in QR-code:



OTP Demo Page

Links

- Go to public page
- Go to protected page
- logout (requires JS, due to Basic auth)

Environment

URI	/protected/
User	maggie

Prepared Users

User	OTP Kind	QR Code	Tools

maggie	TOTP (Time)
	Digits: 6
	Period: 30 seconds
			OTP via `oathtool`:
			`oathtool --totp a4d8acbddef654fccc418db4cc2f85cea6339f00`
			
			Data in QR-code:
			`otpauth://totp/OTPDemo%3Amaggie?secret=utmkzpo66zkpztcbrw2myl4fz2tdhhya&issuer=OTPDemo`

homer	TOTP (Time) Digits: 8		OTP via `oathtool`: `oathtool --digits=8 --time-step-size=60s --totp 98d63836f833e8e33f9344bf3b912af9fb822c8b`

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Accessibility Hilfe

OTP Demo Page

otp.quelltextlich.at

Suchen

OTP Demo Page

Links

- Go to public page
- Go to protected page

Environment

URI	/
User	*not authenticated*

Prepared Users

User	OTP Kind	QR Code	Tools

maggie	TOTP (Time)
	Digits: 6
	Period: 30 seconds
			OTP via `oathtool`:
			`oathtool --totp a4d8acbddef654fccc418db4cc2f85cea6339f00`
			
			Data in QR-code:
			`otpauth://totp/OTPDemo%3Amaggie?secret=utmkzpo66zkpztcbrw2myl4fz2tdhhya&issuer=OTPDemo`

homer	TOTP (Time) Digits: 8 Period: 60 seconds		OTP via `oathtool`: `oathtool --digits=8 --time-step-size=60s --totp 98d63836f833e8e33f9344bf3b912af9fb822c8b` Data in QR-code:

Demo

- Ein OATH HOTP/TOPT Programm installieren
  - Computer: sudo apt-get oathtool
  - Smartphone: Google Authenticator

- http://otp.quelltextlich.at/

- Für Benutzer 'maggie'

  oathtool --totp a4d8acbddef654fccc418db4cc2f85cea6339f00

  → 445552

Folien: http://otp.quelltextlich.at/fhlug.pdf

Further systems

- OTPW
  - 1997, RIPEMD-160
- One time passwords in everything (OPIE)
  - ?, MD4/MD5
- Business focus
  - RSA SecurID
  - YubiCloud OTP
- General 2FA
  - U2F (FIDO. YubiKeys. Usable for GitHub, Dropbox, Google, ...)

- Wikipedia (de): Zwei-Faktor-Authentifizierung
- Wikipedia (en): Two-factor Authentication
- Wikipedia (en): Multi-factor Authentication

- RFC 1760: The S/KEY One-Time Password System
- RFC 1938: A One-Time Password System
- RFC 2243: OTP Extended Responses
- RFC 2289: A One-Time Password System
- RFC 2444: The One-Time-Password SASL Mechanism
- RFC 4226: HOTP: An HMAC-Based One-Time Password Algorithm
- RFC 4648: The Base16, Base32, and Base64 Data Encodings
- RFC 6238: TOTP: Time-Based One-Time Password Algorithm
- Mobile-OTP (mOTP)
- RSA SecurID
- One time password is everything (OPIE)
- OTPW

- Initiative for Open Authentication
- oath-toolkit
- Google Authenticator (OTP App für Android, iPhone)
- Google Authenticator Open Source (F-Droid)
- FreeOTP App (F-Droid)

- LinOTP
- privacyIDEA
- YubiCloud OTP