PortuLock: OpenPGP Keyserver for Organizations

ERIK ESCHER 33443

MASTER THESIS

2021-12-07

PROF. EGGENDORFER

PROF. PFEIL

Motivation

Privacy Preserving Key Distribution

- Centralized Keyservers
- Manual exchanges

Verifying Keys and Identities

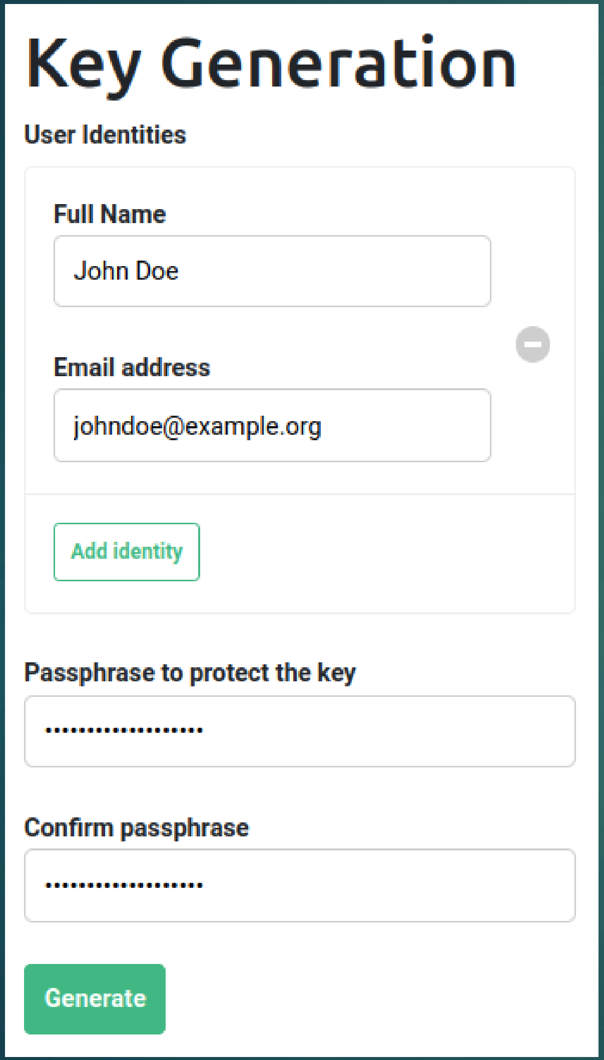
- Hard
- Inconvenient
- Often ignored or postponed

Unlimited Trust in many CAs

Goals

- Ease of Use
- Delegating Verification
- Federation
- Privacy Preserving
- Suitable for Organizations
- Authoritative
- Interoperability

Key Generation



Key Generation

User Identities

Full Name

John Doe

Email address

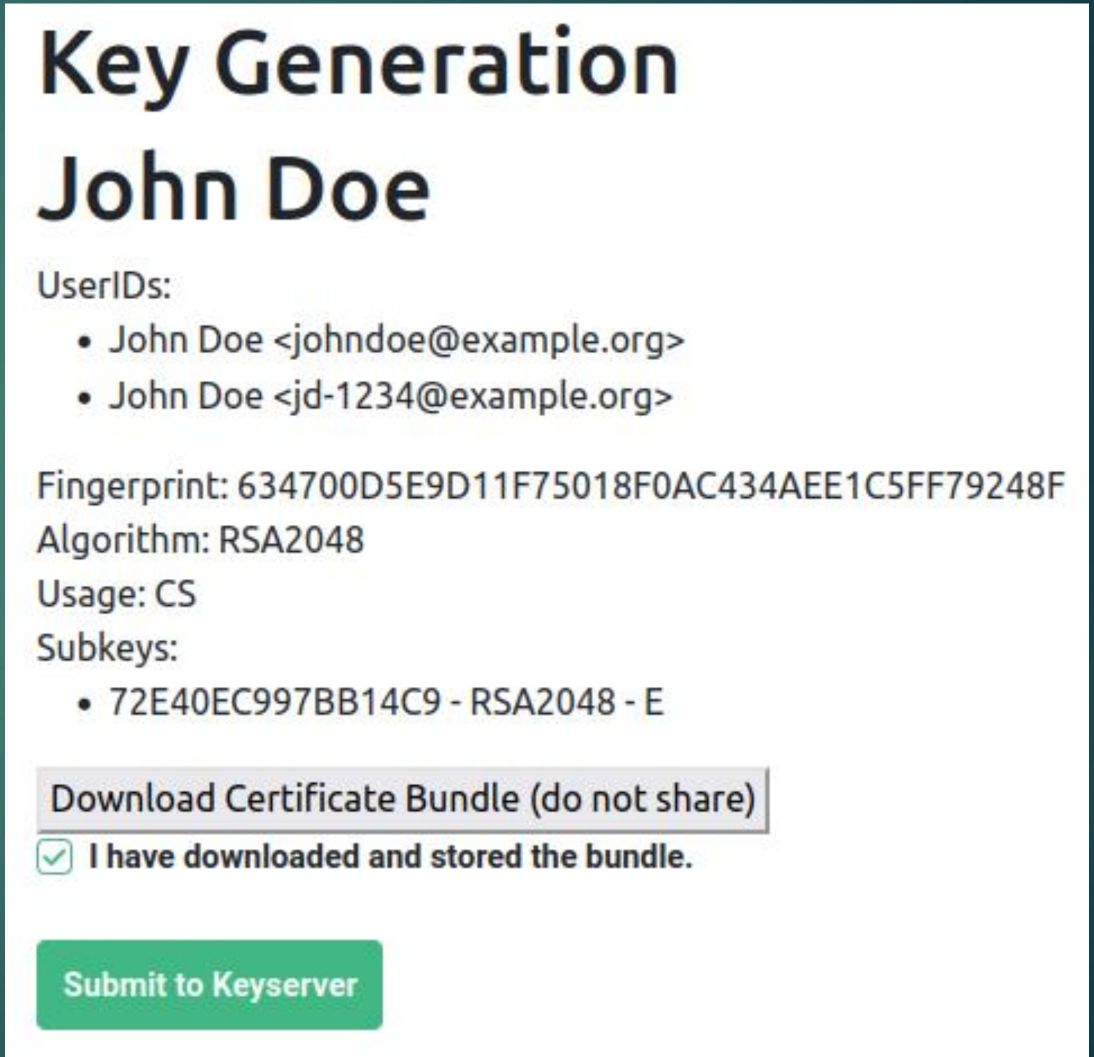
johndoe@example.org

Passphrase to protect the key

••••••••••••••••••

Confirm passphrase

••••••••••••••••••



Key Generation

John Doe

UserIDs:

- John Doe <johndoe@example.org>
- John Doe <jd-1234@example.org>

Fingerprint: 634700D5E9D11F75018F0AC434AEE1C5FF79248F

Algorithm: RSA2048

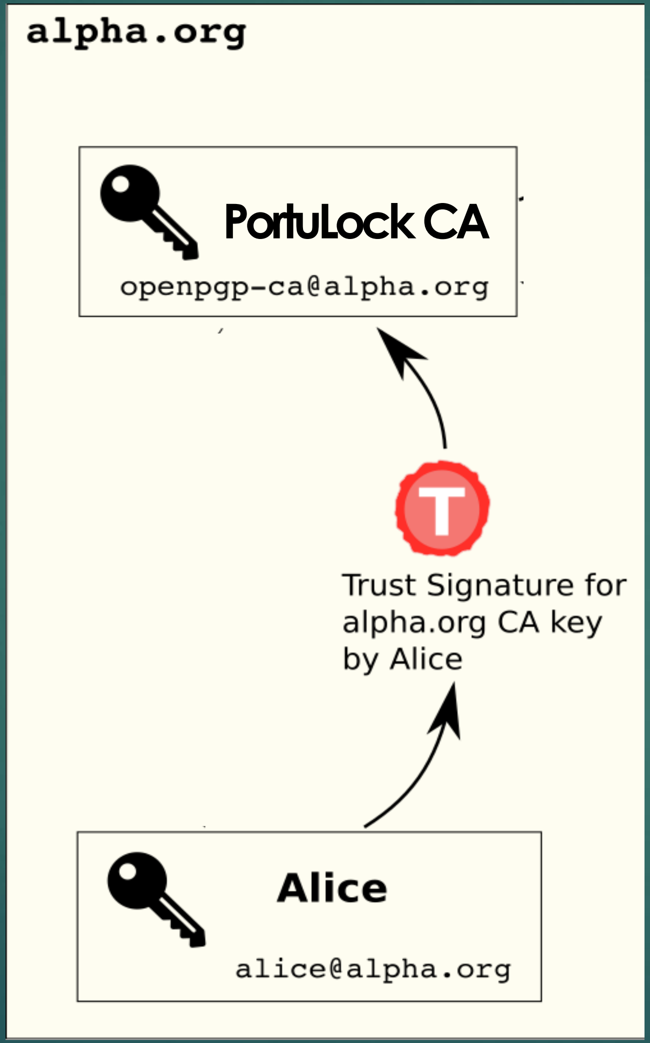
Usage: CS

Subkeys:

- 72E40EC997BB14C9 - RSA2048 - E

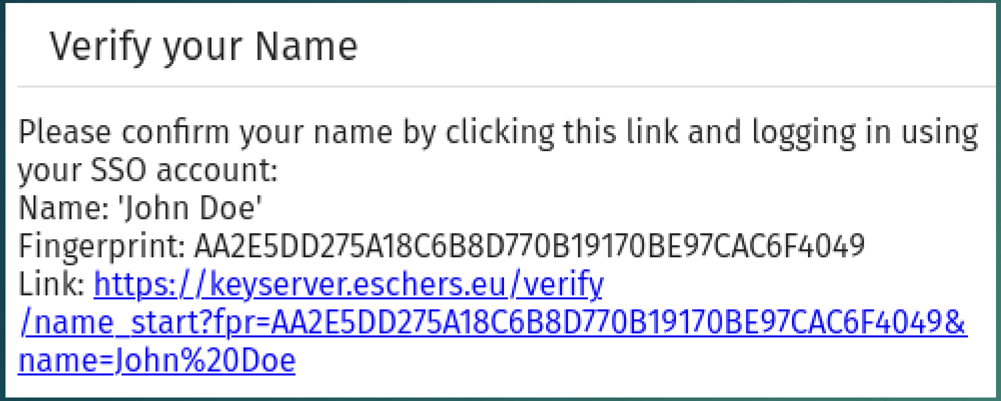
☑ I have downloaded and stored the bundle.

Trust Signature



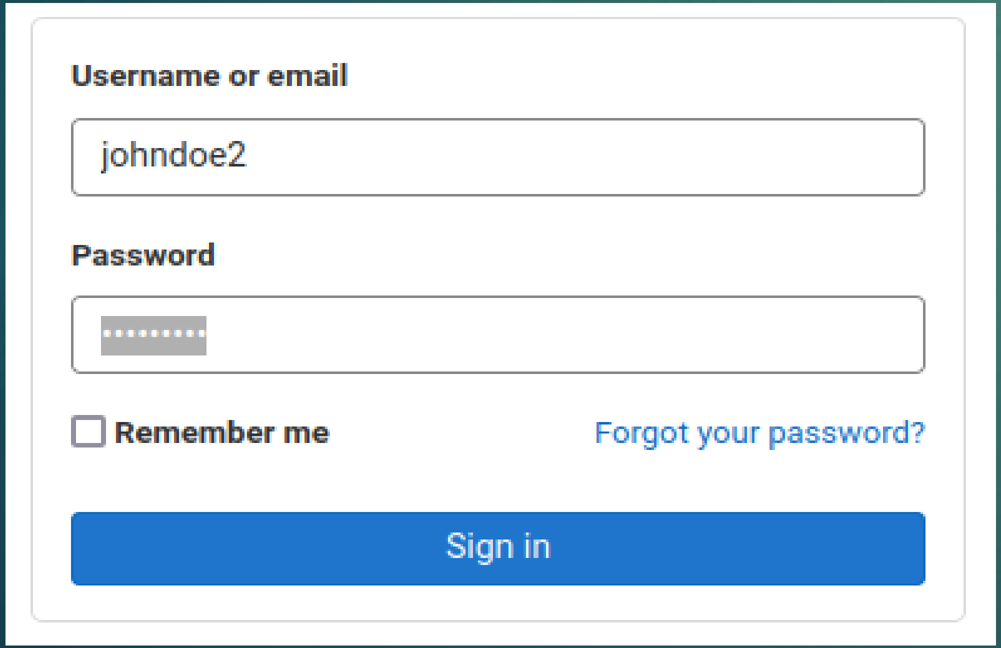
Source (modified):
OpenPGP-CA Project
CC-BY 4.0, see [2]

Identity Verification



Verify your Name

Please confirm your name by clicking this link and logging in using your SSO account:
Name: 'John Doe'
Fingerprint: AA2E5DD275A18C6B8D770B19170BE97CAC6F4049
Link: https://keyserver.eschers.eu/verify/name_start?fpr=AA2E5DD275A18C6B8D770B19170BE97CAC6F4049&name=John%20Doe



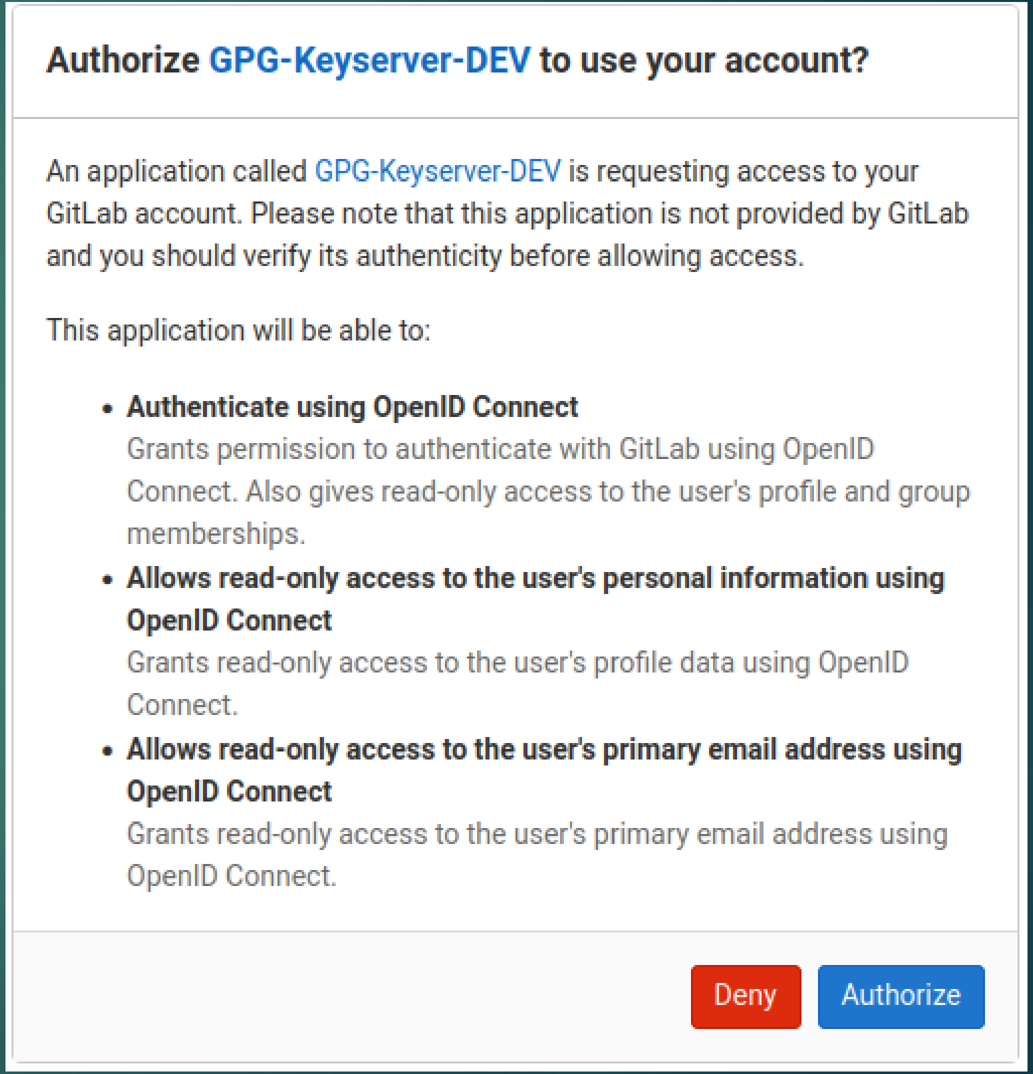
Username or email

johndoe2

Password

••••••••••

□ **Remember me**



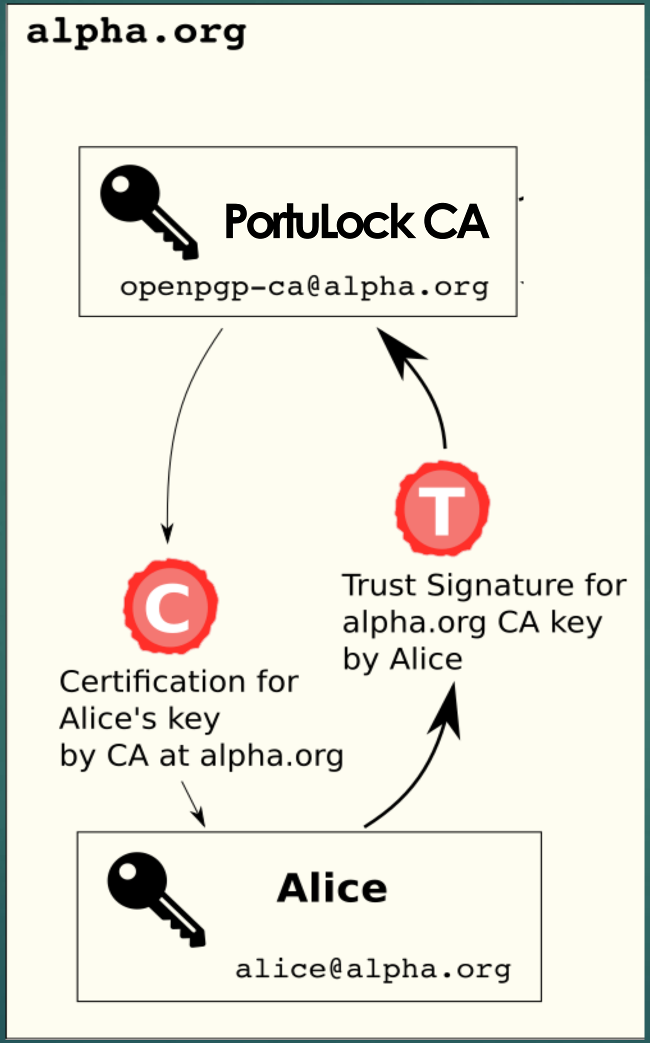
Authorize GPG-Keyserver-DEV to use your account?

An application called GPG-Keyserver-DEV is requesting access to your GitLab account. Please note that this application is not provided by GitLab and you should verify its authenticity before allowing access.

This application will be able to:

- **Authenticate using OpenID Connect**
  Grants permission to authenticate with GitLab using OpenID Connect. Also gives read-only access to the user's profile and group memberships.
- **Allows read-only access to the user's personal information using OpenID Connect**
  Grants read-only access to the user's profile data using OpenID Connect.
- **Allows read-only access to the user's primary email address using OpenID Connect**
  Grants read-only access to the user's primary email address using OpenID Connect.

Certification



Source (modified):
OpenPGP-CA Project
CC-BY 4.0, see [2]

Publishing and Locating Keys

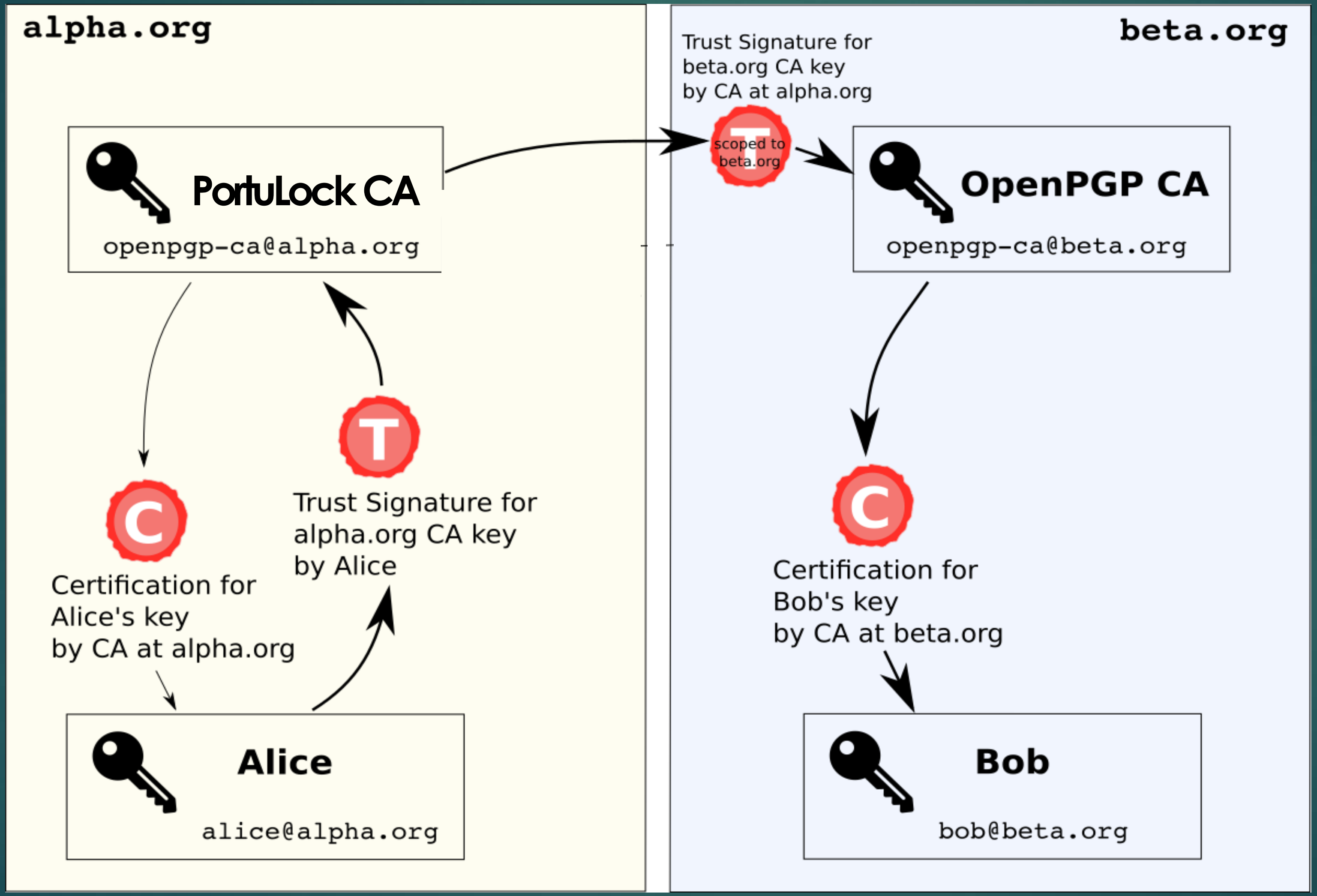
Web Key Discovery

- Federated, Authoritative
- https://openpgpkey.<domain>/<...>/<hashed-localpart-from-email>
- Supported by Clients

Aggregation Feature

- Granular Configuration based on Mail Domains
- Delegating Trust and Verification
- Simplified validation of external keys
- Keyserver Proxy

Federated Trust (OpenPGP-CA)



Source (modified):
OpenPGP-CA Project
CC-BY 4.0, see [2]

Conclusion

- ✓ Makes OpenPGP usable for organizations
- Improves practical key verification
- Preserves Privacy
- https://gitlab.com/portulock
- Outlook: Adoption of Digital Signatures

Thanks for your attention!

Questions?

[1]

Sources

All sources last checked on 2021-12-03
(unless marked otherwise)

- [1] https://office.microsoft.com/de-de/images/results.aspx?qu=00423171.wmf&ex=2#ai:MC900423171, last checked on 2013-07-01
- [2] https://openpgp-ca.org/background/details/

Backup-Slides

PortuLock Name

Portulak

[B2]

Portunus

- Roman God of "keys, doors, livestock and ports" [B1]
-

[B3]

Sources: (last checked 2021-12-06)
[B1] https://en.wikipedia.org/wiki/Portunus_(mythology)
[B2] https://www.mein-schoener-garten.de/pflanzen/portulak/portulakroeschen
[B3] https://commons.wikimedia.org/wiki/File:TempleOfPortunus-ForumBoarium.jpg

Motivation

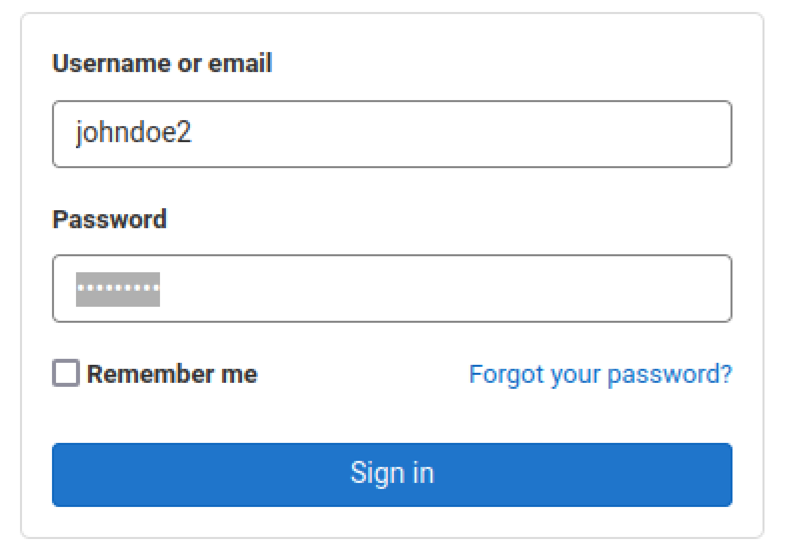
Asymmetric Cryptography

- Integrity, Authenticity, Non-Repudiation
- Confidentiality

Applications

- Replacing paper-based signatures
- Robust, secure communication even without trusted infrastructure (Disaster Recovery)
- Additional protection for mail (Spoofing, Phishing, compromised servers)

Identity Verification



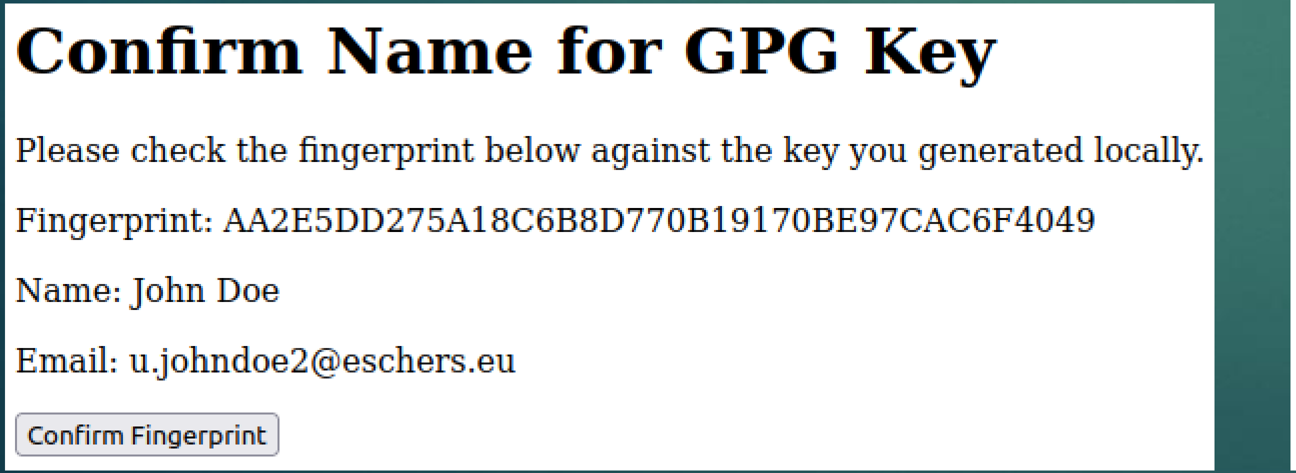
Username or email

johndoe2

Password

•••••••••

□ Remember me



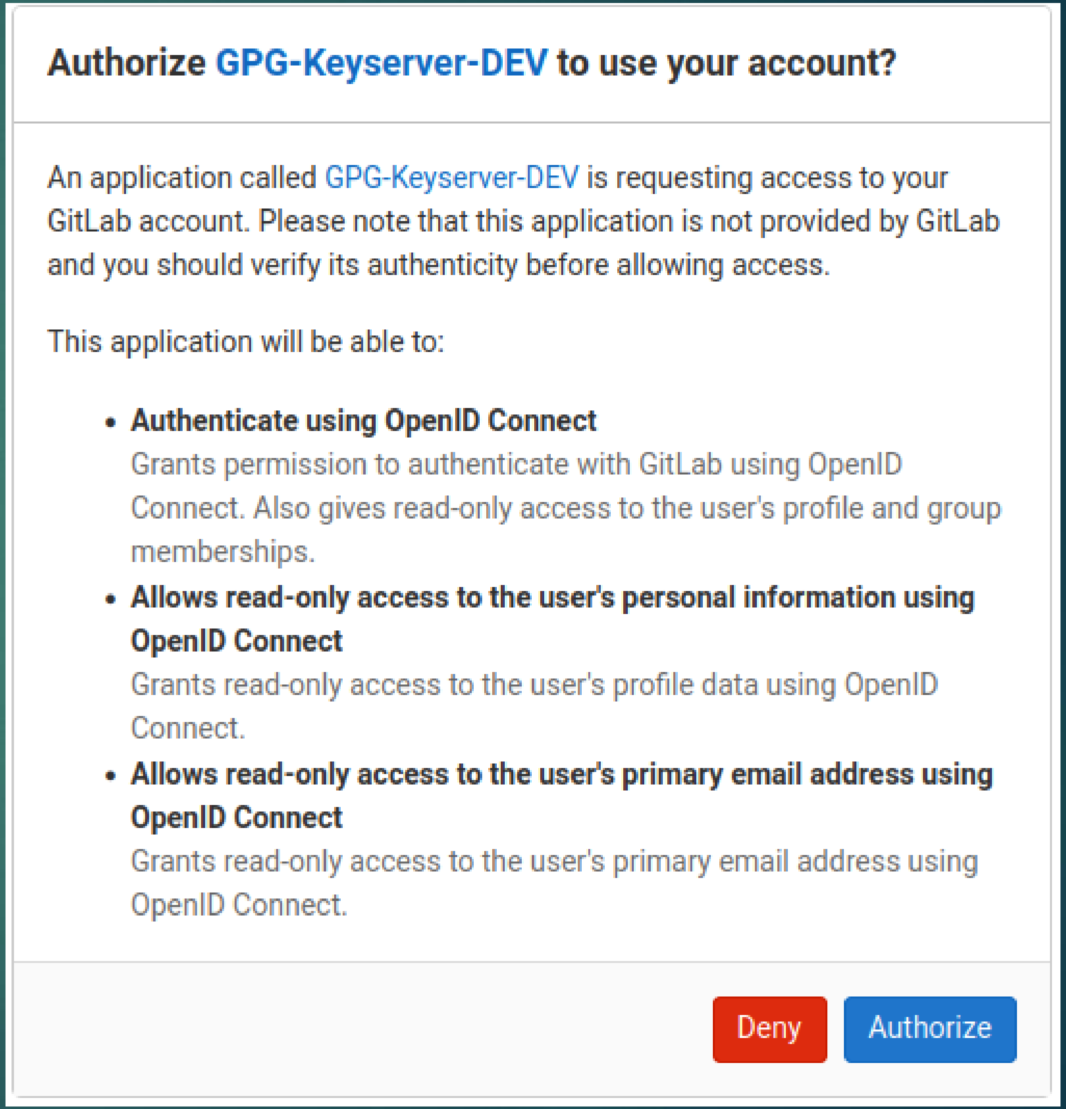
Confirm Name for GPG Key

Please check the fingerprint below against the key you generated locally.

Fingerprint: AA2E5DD275A18C6B8D770B19170BE97CAC6F4049

Name: John Doe

Email: u.johndoe2@eschers.eu



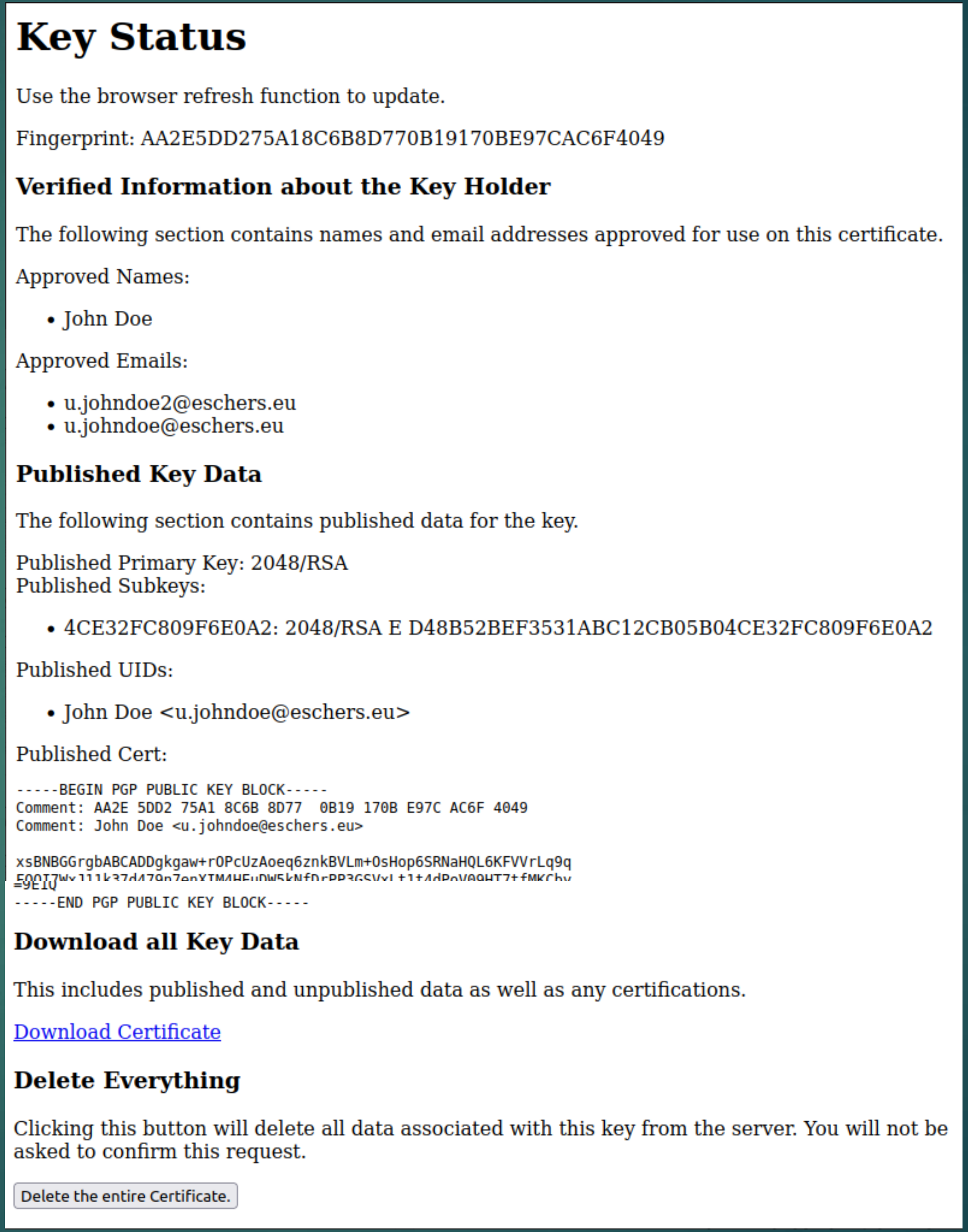
Authorize GPG-Keyserver-DEV to use your account?

An application called GPG-Keyserver-DEV is requesting access to your GitLab account. Please note that this application is not provided by GitLab and you should verify its authenticity before allowing access.

This application will be able to:

- **Authenticate using OpenID Connect**
  Grants permission to authenticate with GitLab using OpenID Connect. Also gives read-only access to the user's profile and group memberships.
- **Allows read-only access to the user's personal information using OpenID Connect**
  Grants read-only access to the user's profile data using OpenID Connect.
- **Allows read-only access to the user's primary email address using OpenID Connect**
  Grants read-only access to the user's primary email address using OpenID Connect.

Status, Deletion



Key Status

Use the browser refresh function to update.

Fingerprint: AA2E5DD275A18C6B8D770B19170BE97CAC6F4049

Verified Information about the Key Holder

The following section contains names and email addresses approved for use on this certificate.

Approved Names:

- John Doe

Approved Emails:

- u.johndoe2@eschers.eu
- u.johndoe@eschers.eu

Published Key Data

The following section contains published data for the key.

Published Primary Key: 2048/RSA
Published Subkeys:

- 4CE32FC809F6E0A2: 2048/RSA E D48B52BEF3531ABC12CB05B04CE32FC809F6E0A2

Published UIDs:

- John Doe <u.johndoe@eschers.eu>

Published Cert:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: AA2E 5DD2 75A1 8C6B 8D77  0B19 170B E97C AC6F 4049
Comment: John Doe <u.johndoe@eschers.eu>

xsBNBGGrgbABCADDgkgaw+rOPcUzAoeq6znkBVLm+OsHop6SRNaHQL6KFVVrLq9q
E0OI7Wx111k37d479p7epXIM4HFuDW5kNfDrPP3GSVxLt1t4dPoV09HT7tfMKCby
=9EIQ
-----END PGP PUBLIC KEY BLOCK-----
```

Download all Key Data

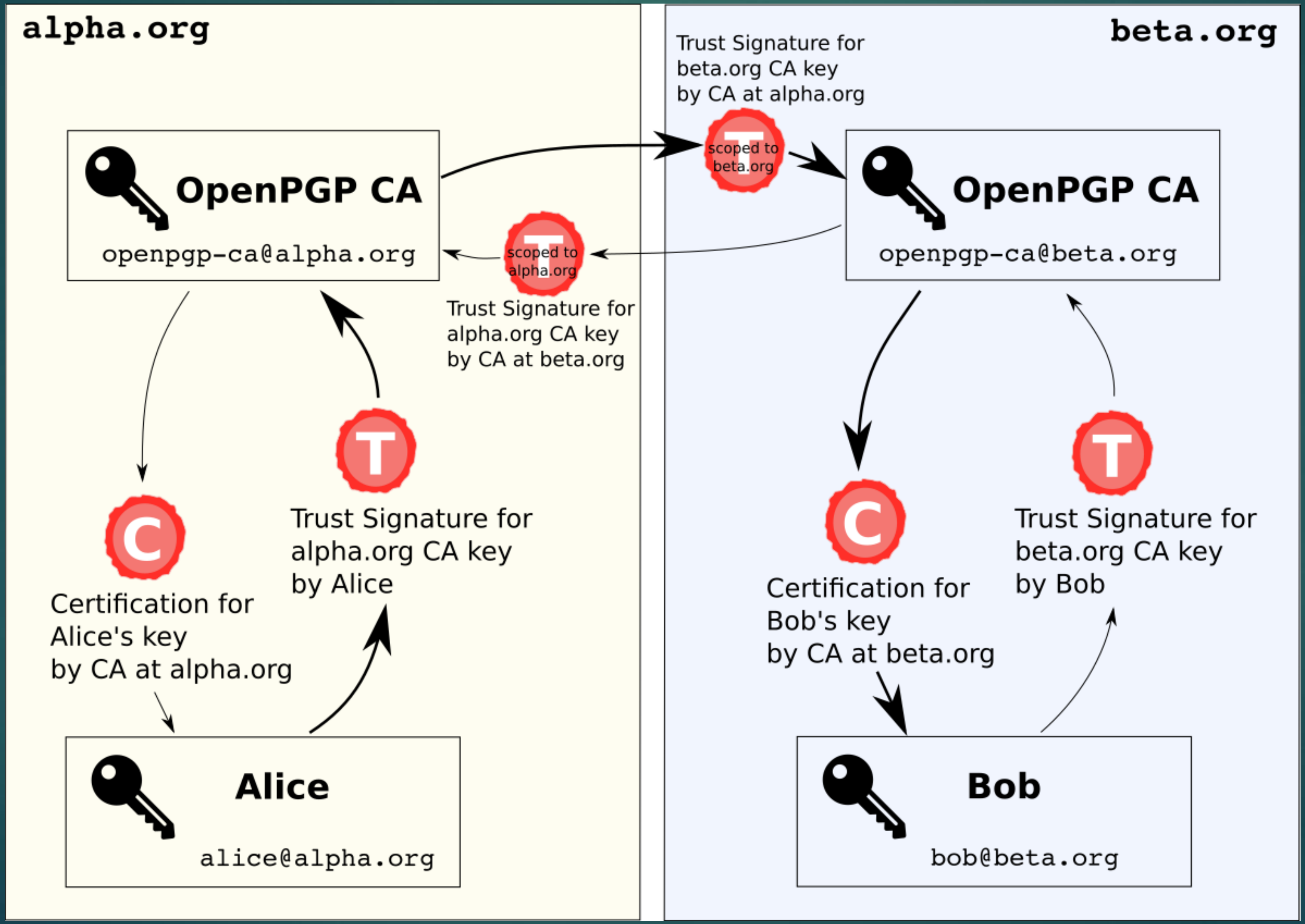
This includes published and unpublished data as well as any certifications.

Download Certificate

Delete Everything

Clicking this button will delete all data associated with this key from the server. You will not be asked to confirm this request.

OpenPGP-CA Trust Model



Source (unmodified):
OpenPGP-CA Project
CC-BY 4.0, see [2]