gwcert

Andrew Schweitzer

Aug 15, 2023

CONTENTS

Tools for creating TLS certificates for use with, e.g. MQTT and RabbitMQ.

NOTE: these are temporary tools for *non-production* deployments. This library is more or less equivalent to a README containing OpenSSL commands, but less manual.

This library is a thin wrapper around ownca, which wraps pyca/cryptography, which wraps the OpenSSL C library. See also tls-gen, a repo from rabbitmq, which performs a similar task using a stack of make/python/OpenSSL CLI.

CHAPTER

ONE

FEATURES

- Create a local Certificate Authority directory with a self-signed certificate, via `gwcert ca create`.
- Create named key pairs, CSRs and certificates with *arbitrary* input and output paths, via `gwcert key add`.
- Build cli commands visually with `gwcert tui`.

CHAPTER

TWO

INSTALLATION

The recommended way to install *gwcert* is with pipx from PyPI:

```
$ pipx install gridworks-cert
```

CHAPTER

THREE

USAGE

Get help with any of:

```
gwcert
gwcert ca
gwcert key
```

Create a Certificate Authority directory with a self-signed certificate via:

```
gwcert ca create
```

Show information about the locally created ca and keys with:

```
gwcert ca info
```

Add a named set of keys (public, private, certificate) via, for example:

```
gwcert key add KEY_NAME
```

Show information about a certificate:

```
gwcert key info KEY_NAME
```

Build CLI commands visually:

```
gwcert tui
```

Please see the *Command-line Reference* for more details.

CHAPTER

FOUR

CONTRIBUTING

Contributions are very welcome. To learn more, see the *Contributor Guide*.

CHAPTER

FIVE

LICENSE

Distributed under the terms of the *MIT license*, *gwcert* is free and open source software.

CHAPTER

SIX

ISSUES

If you encounter any problems, please file an issue along with a detailed description.

CHAPTER

SEVEN

CREDITS

This project was generated from @cjolowicz's Hypermodern Python Cookiecutter template.

7.1 Usage

7.1.1 gwcert

GridWords TLS certificate tools.

```
gwcert [OPTIONS] COMMAND [ARGS]...
```

Options

--version

Show version and exit.

Default
`False`

--install-completion <install_completion>

Install completion for the specified shell.

Options
bash | zsh | fish | powershell | pwsh

--show-completion <show_completion>

Show completion for the specified shell, to copy it or customize the installation.

Options
bash | zsh | fish | powershell | pwsh

ca

Commands for creating and using a local Certificate Authority.

```
gwcert ca [OPTIONS] COMMAND [ARGS]...
```

add-key

Generate public/private key pair, CSR and signed certificate.

```
gwcert ca add-key [OPTIONS] KEY_NAME
```

Options

--ca-dir <ca_dir>

CA storage directory.

Default
/home/docs/.local/share/gridworks/ca

--force

Overwrites existing files. [yellow][bold]WARNING: [/yellow][/bold]–force will [red][bold]PERMANENTLY DELETE[/red][/bold] the files for this key name, including public and private key.

Default
False

--valid-days <valid_days>

Number of days issued certificates should be valid for

Default
825

--public-exponent <public_exponent>

Passed to cryptography.hazmat.primitives.asymmetric.rsa.generate_private_key()

Default
65537

--key-size <key_size>

Passed to cryptography.hazmat.primitives.asymmetric.rsa.generate_private_key()

Default
2048

--common-name <common_name>

Common Name used in certificate. If unspecified, key-name is used.

Default

--dns <dns_names>

DNS entries

--is-ca

Whether certificate for this key can itself sign other certificates

Default
False

Arguments

KEY_NAME
Required argument

clean

Delete the CA storage directory and contents. [yellow][bold] WARNING: [red] PERMANENTLY DELETES CA CERTIFICATE AND KEY.

```
gwcert ca clean [OPTIONS]
```

Options

--ca-dir <ca_dir>
CA storage directory.

Default
/home/docs/.local/share/gridworks/ca

--yes-really-forever
Required to actually clean the CA storage directory

Default
False

create

Create files necessary for a simple, self-signed Certificate Authority.

```
gwcert ca create [OPTIONS] COMMON_NAME
```

Options

--ca-dir <ca_dir>
CA storage directory.

Default
/home/docs/.local/share/gridworks/ca

--valid-days <valid_days>
Number of days issued certificates should be valid for

Default
825

--public-exponent <public_exponent>

Passed to cryptography.hazmat.primitives.asymmetric.rsa.generate_private_key()

Default
65537

--key-size <key_size>

Passed to cryptography.hazmat.primitives.asymmetric.rsa.generate_private_key()

Default
2048

Arguments

COMMON_NAME

Required argument

info

Show information about CA configured on disk.

```
gwcert ca info [OPTIONS]
```

Options

--ca-dir <ca_dir>

CA storage directory.

Default
/home/docs/.local/share/gridworks/ca

key

Commands for generating named keys, Certificate Signing Requests and Certificates.

By default certificates are generated in:

$HOME/.local/share/gridworks/ca/certs/KEYNAME/

By default CA files are:

$HOME/.local/share/gridworks/ca/ca.crt $HOME/.local/share/gridworks/ca/private/ca_key.pem.

Subcommands rsa, csr and certify may be called in order to produce key/certificate pairs usable with the specified CA. Subcommand 'add' calls all three of those in order.

The I/O of these commands is approximately:

rsa -> private key csr(private key) -> CSR certify(CSR, CA certificate, CA private key) -> certificate

```
gwcert key [OPTIONS] COMMAND [ARGS]...
```

add

Generate public/private RSA key pair, CSR and certificate for a named identity.

Writes public/private key, CSR and certificate files, by default named:

$HOME/.local/share/gridworks/ca/certs/name/name.pub $HOME/.local/share/gridworks/ca/certs/name/private/name.pem
$HOME/.local/share/gridworks/ca/certs/name/name.csr $HOME/.local/share/gridworks/ca/certs/name/name.crt

Input file can be explicitly named with the –ca-certificate-path and –ca-private-key-path parameters. Output file can be explicitly named by passing a path-like string for a ".pem" file to the name parameter and/or with –csr-path and –certificate-path parameters.

```
gwcert key add [OPTIONS] NAME
```

Options

--csr-path <csr_path>

Optional explicit path to Certificate Signing Request. If absent, CSR path is derived from the private key output path.

--private-key-path <private_key_path>

Optional explicit path to private key. If absent, private key path is derived from the certificate output path.

--certs-dir <certs_dir>

Base storage directory for named certs

Default
`/home/docs/.local/share/gridworks/ca/certs`

--public-exponent <public_exponent>

The public exponent of the new key. Either 65537 or 3 (for legacy purposes). Almost everyone should use 65537.

Default
`65537`

--key-size <key_size>

The length of the modulus in bits. It is strongly recommended to be at least 2048.

Default
`2048`

--force

Overwrites existing files. [yellow][bold]WARNING: [/yellow][/bold]–force will [red][bold]PERMANENTLY DELETE[/red][/bold] the public and private key for this key name

Default
`False`

--common-name <common_name>

Common Name used in certificate. If unspecified, key-name is used.

Default

--dns <dns_names>

DNS entries

--ca-certificate-path <ca_certificate_path>

Optional explicit path to CA certificate file. If absent, CA certificate path is derived from ca_dir.

--ca-private-key-path <ca_private_key_path>

Optional explicit path to CA private key file. If absent, CA private key path is derived from ca_dir.

--ca-dir <ca_dir>

Certificate Authority directory

Default
/home/docs/.local/share/gridworks/ca

--valid-days <valid_days>

Number of days issued certificates should be valid for

Default
825

Arguments

NAME

Required argument

certify

Sign a CSR, producing a certificate.

Uses input files, by default named:

$HOME/.local/share/gridworks/ca/certs/name/name.csr

Writes a certificate file, by default named:

$HOME/.local/share/gridworks/ca/certs/name/name.crt

Input file can be explicitly named with the –csr-path, –ca-certificate-path and –ca-private-key-path parameters. Output file can be explicitly named by passing a path-like string for a ".crt" file to the name parameter.

```
gwcert key certify [OPTIONS] NAME
```

Options

--csr-path <csr_path>

Optional explicit path to Certificate Signing Request. If absent, CSR path is derived from thecertificate output path.

--ca-certificate-path <ca_certificate_path>

Optional explicit path to CA certificate file. If absent, CA certificate path is derived from ca_dir.

--ca-private-key-path <ca_private_key_path>

Optional explicit path to CA private key file. If absent, CA private key path is derived from ca_dir.

--ca-dir <ca_dir>

Certificate Authority directory

Default
/home/docs/.local/share/gridworks/ca

--certs-dir <certs_dir>

Base storage directory for named certs

Default
/home/docs/.local/share/gridworks/ca/certs

--valid-days <valid_days>

Number of days issued certificates should be valid for

Default
825

--force

Overwrites existing certificate file. [yellow][bold]WARNING: [/yellow][/bold]–force will [red][bold]PERMANENTLY DELETE[/red][/bold] the certificate file for this name

Default
False

Arguments

NAME

Required argument

csr

Create Certificate Signing Request from a private key.

Uses input files, by default named:

$HOME/.local/share/gridworks/ca/certs/name/private/name.pem

Writes a CSR file, by default named:

$HOME/.local/share/gridworks/ca/certs/name/name.csr

Input file can be explicitly named with the –private-key-path paramter. Output file can be explicitly named by passing a path-like string for a ".csr" file to the name parameter.

```
gwcert key csr [OPTIONS] NAME
```

Options

--private-key-path <private_key_path>

Optional explicit path to private key file. If absent, private key path is derived from csr output path.

--certs-dir <certs_dir>

Base storage directory for named certs

Default
/home/docs/.local/share/gridworks/ca/certs

--common-name <common_name>

Common Name used in certificate. If unspecified, key-name is used.

Default

--dns <dns_names>

DNS entries

--force

Overwrites existing file. [yellow][bold]WARNING: [/yellow][/bold]–force will [red][bold]PERMANENTLY DELETE[/red][/bold] the csr file for this name

Default
False

Arguments

NAME

Required argument

info

Show information about a certificate using '[cyan]openssl x509 -in CERTIFICATE_PATH -text -noout[/cyan]'.

```
gwcert key info [OPTIONS] NAME
```

Options

--certs-dir <certs_dir>

Base storage directory for named certs

Default
/home/docs/.local/share/gridworks/ca/certs

--files

Show paths of files in directory of certificate.

Default
False

Arguments

NAME

Required argument

rsa

Create public/private key pair using RSA.

Writes public and private key files, by default named:

$HOME/.local/share/gridworks/ca/certs/name/name.pub $HOME/.local/share/gridworks/ca/certs/name/private/name.pem

Output files can be explicitly named by passing a path-like string for a ".pem" file to the name parameter.

```
gwcert key rsa [OPTIONS] NAME
```

Options

--private-key-path <private_key_path>

Optional explicit path to private key file. If absent, private key path is derived from public key output path.

--certs-dir <certs_dir>

Base storage directory for named certs

Default

`/home/docs/.local/share/gridworks/ca/certs`

--public-exponent <public_exponent>

The public exponent of the new key. Either 65537 or 3 (for legacy purposes). Almost everyone should use 65537.

Default

`65537`

--key-size <key_size>

The length of the modulus in bits. It is strongly recommended to be at least 2048.

Default

`2048`

--force

Overwrites existing files. [yellow][bold]WARNING: [/yellow][/bold]–force will [red][bold]PERMANENTLY DELETE[/red][/bold] the public and private key for this key name

Default

`False`

Arguments

NAME
Required argument

tui

Visual CLI command builder.

```
gwcert tui [OPTIONS]
```

7.2 Reference

7.2.1 gwcert

gwcert package.

gwcert.ca

Exports for gwcert.ca package.

7.3 Contributor Guide

Thank you for your interest in improving this project. This project is open-source under the MIT license and welcomes contributions in the form of bug reports, feature requests, and pull requests.

Here is a list of important resources for contributors:

- Source Code
- Documentation
- Issue Tracker
- *Code of Conduct*

7.3.1 How to report a bug

Report bugs on the Issue Tracker.

When filing an issue, make sure to answer these questions:

- Which operating system and Python version are you using?
- Which version of this project are you using?
- What did you do?
- What did you expect to see?
- What did you see instead?

The best way to get your bug fixed is to provide a test case, and/or steps to reproduce the issue.

7.3.2 How to request a feature

Request features on the Issue Tracker.

7.3.3 How to set up your development environment

You need Python 3.7+ and the following tools:

- Poetry
- Nox
- nox-poetry

Install the package with development requirements:

```
$ poetry install
```

You can now run an interactive Python session, or the command-line interface:

```
$ poetry run python
$ poetry run gridworks-cert
```

7.3.4 How to test the project

Run the full test suite:

```
$ nox
```

List the available Nox sessions:

```
$ nox --list-sessions
```

You can also run a specific Nox session. For example, invoke the unit test suite like this:

```
$ nox --session=tests
```

Unit tests are located in the *tests* directory, and are written using the pytest testing framework.

7.3.5 How to submit changes

Open a pull request to submit changes to this project.

Your pull request needs to meet the following guidelines for acceptance:

- The Nox test suite must pass without errors and warnings.
- Include unit tests. This project maintains 100% code coverage.
- If your changes add functionality, update the documentation accordingly.

Feel free to submit early, though—we can always iterate on this.

To run linting and code formatting checks before committing your change, you can install pre-commit as a Git hook by running the following command:

```
$ nox --session=pre-commit -- install
```

It is recommended to open an issue before starting work on anything. This will allow a chance to talk it over with the owners and validate your approach.

7.4 Contributor Covenant Code of Conduct

7.4.1 Our Pledge

We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone, regardless of age, body size, visible or invisible disability, ethnicity, sex characteristics, gender identity and expression, level of experience, education, socio-economic status, nationality, personal appearance, race, caste, color, religion, or sexual identity and orientation.

We pledge to act and interact in ways that contribute to an open, welcoming, diverse, inclusive, and healthy community.

7.4.2 Our Standards

Examples of behavior that contributes to a positive environment for our community include:

- Demonstrating empathy and kindness toward other people
- Being respectful of differing opinions, viewpoints, and experiences
- Giving and gracefully accepting constructive feedback
- Accepting responsibility and apologizing to those affected by our mistakes, and learning from the experience
- Focusing on what is best not just for us as individuals, but for the overall community

Examples of unacceptable behavior include:

- The use of sexualized language or imagery, and sexual attention or advances of any kind
- Trolling, insulting or derogatory comments, and personal or political attacks
- Public or private harassment
- Publishing others' private information, such as a physical or email address, without their explicit permission
- Other conduct which could reasonably be considered inappropriate in a professional setting

7.4.3 Enforcement Responsibilities

Community leaders are responsible for clarifying and enforcing our standards of acceptable behavior and will take appropriate and fair corrective action in response to any behavior that they deem inappropriate, threatening, offensive, or harmful.

Community leaders have the right and responsibility to remove, edit, or reject comments, commits, code, wiki edits, issues, and other contributions that are not aligned to this Code of Conduct, and will communicate reasons for moderation decisions when appropriate.

7.4.4 Scope

This Code of Conduct applies within all community spaces, and also applies when an individual is officially representing the community in public spaces. Examples of representing our community include using an official e-mail address, posting via an official social media account, or acting as an appointed representative at an online or offline event.

7.4.5 Enforcement

Instances of abusive, harassing, or otherwise unacceptable behavior may be reported to the community leaders responsible for enforcement at schweitz72@gmail.com. All complaints will be reviewed and investigated promptly and fairly.

All community leaders are obligated to respect the privacy and security of the reporter of any incident.

7.4.6 Enforcement Guidelines

Community leaders will follow these Community Impact Guidelines in determining the consequences for any action they deem in violation of this Code of Conduct:

1. Correction

Community Impact: Use of inappropriate language or other behavior deemed unprofessional or unwelcome in the community.

Consequence: A private, written warning from community leaders, providing clarity around the nature of the violation and an explanation of why the behavior was inappropriate. A public apology may be requested.

2. Warning

Community Impact: A violation through a single incident or series of actions.

Consequence: A warning with consequences for continued behavior. No interaction with the people involved, including unsolicited interaction with those enforcing the Code of Conduct, for a specified period of time. This includes avoiding interactions in community spaces as well as external channels like social media. Violating these terms may lead to a temporary or permanent ban.

3. Temporary Ban

Community Impact: A serious violation of community standards, including sustained inappropriate behavior.

Consequence: A temporary ban from any sort of interaction or public communication with the community for a specified period of time. No public or private interaction with the people involved, including unsolicited interaction with those enforcing the Code of Conduct, is allowed during this period. Violating these terms may lead to a permanent ban.

4. Permanent Ban

Community Impact: Demonstrating a pattern of violation of community standards, including sustained inappropriate behavior, harassment of an individual, or aggression toward or disparagement of classes of individuals.

Consequence: A permanent ban from any sort of public interaction within the community.

7.4.7 Attribution

This Code of Conduct is adapted from the Contributor Covenant, version 2.1, available at https://www.contributor-covenant.org/version/2/1/code_of_conduct.html.

Community Impact Guidelines were inspired by Mozilla's code of conduct enforcement ladder.

For answers to common questions about this code of conduct, see the FAQ at https://www.contributor-covenant.org/faq. Translations are available at https://www.contributor-covenant.org/translations.

7.5 License

PYTHON MODULE INDEX

INDEX

Symbols

C

G

K

M

N