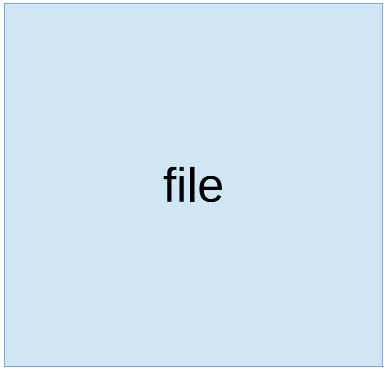
On The Fly Encryption, Compression, Upload To S3

And Back

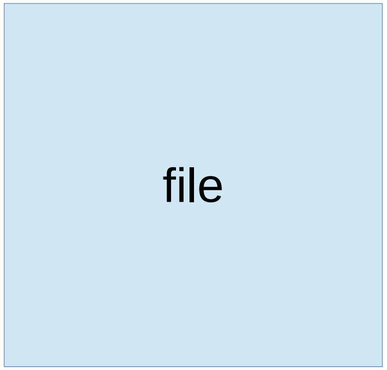
paolo.montrasio@connettiva.eu

connettiva.eu/rubyday2015

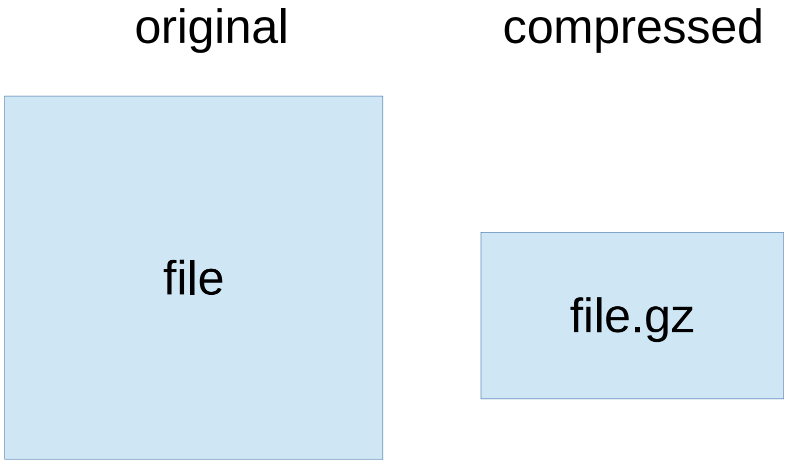
SENSITIVE DATA ON S3?
ENCRYPT ALL THE THINGS!
memegenerator.net



file



file

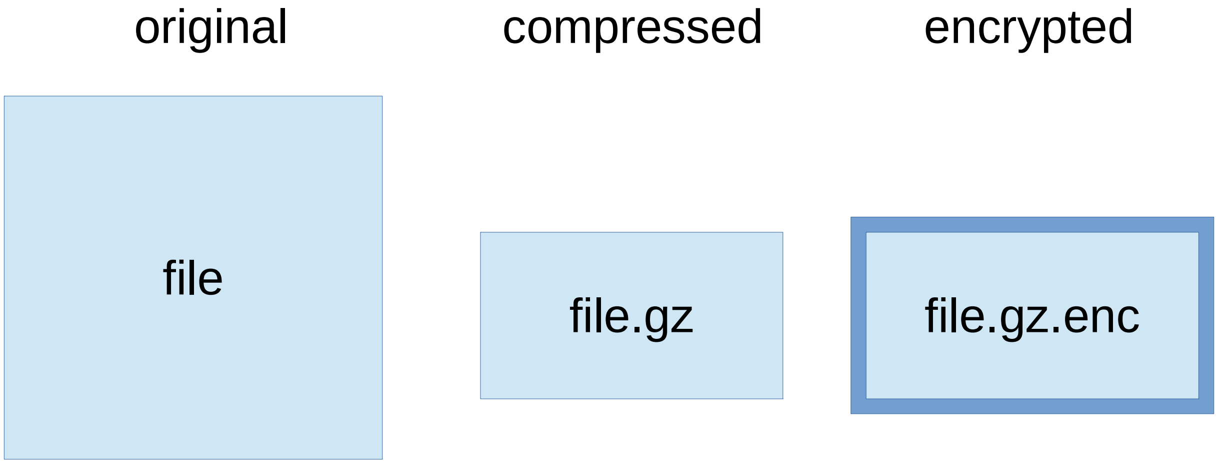


original

compressed

file

file.gz



original

compressed

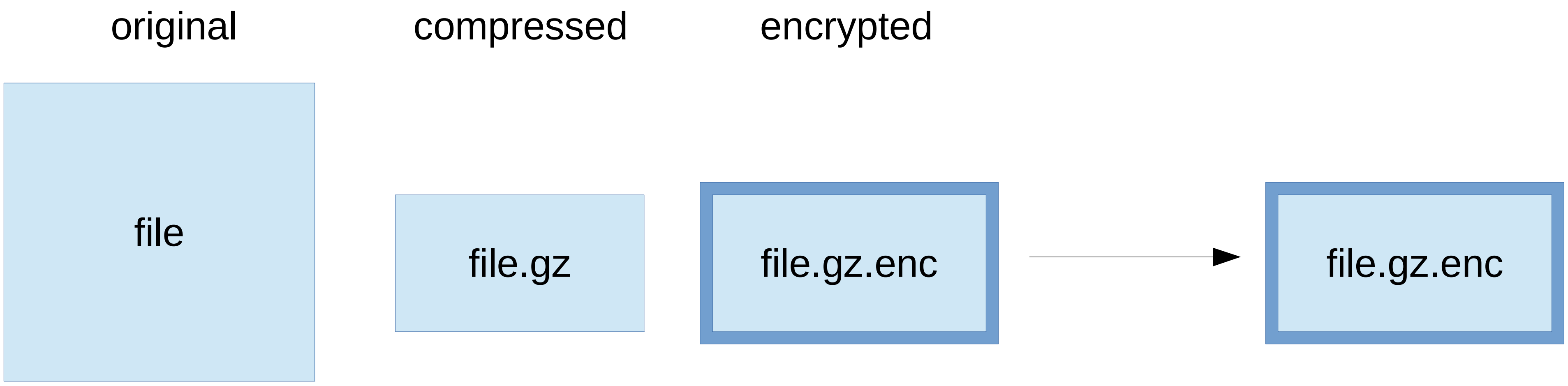
encrypted

file

file.gz

file.gz.enc

S3



original

compressed

encrypted

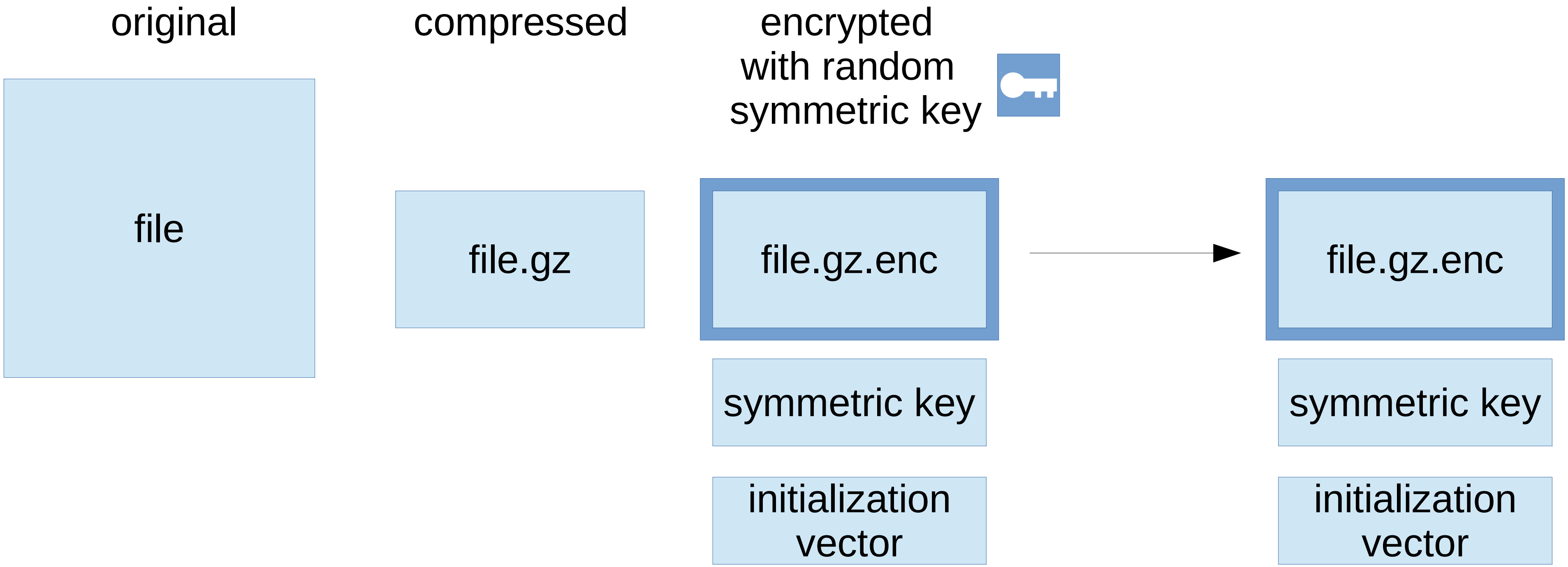
file

file.gz

file.gz.enc

file.gz.enc

S3



original

compressed

encrypted with random symmetric key

file

file.gz

file.gz.enc

symmetric key

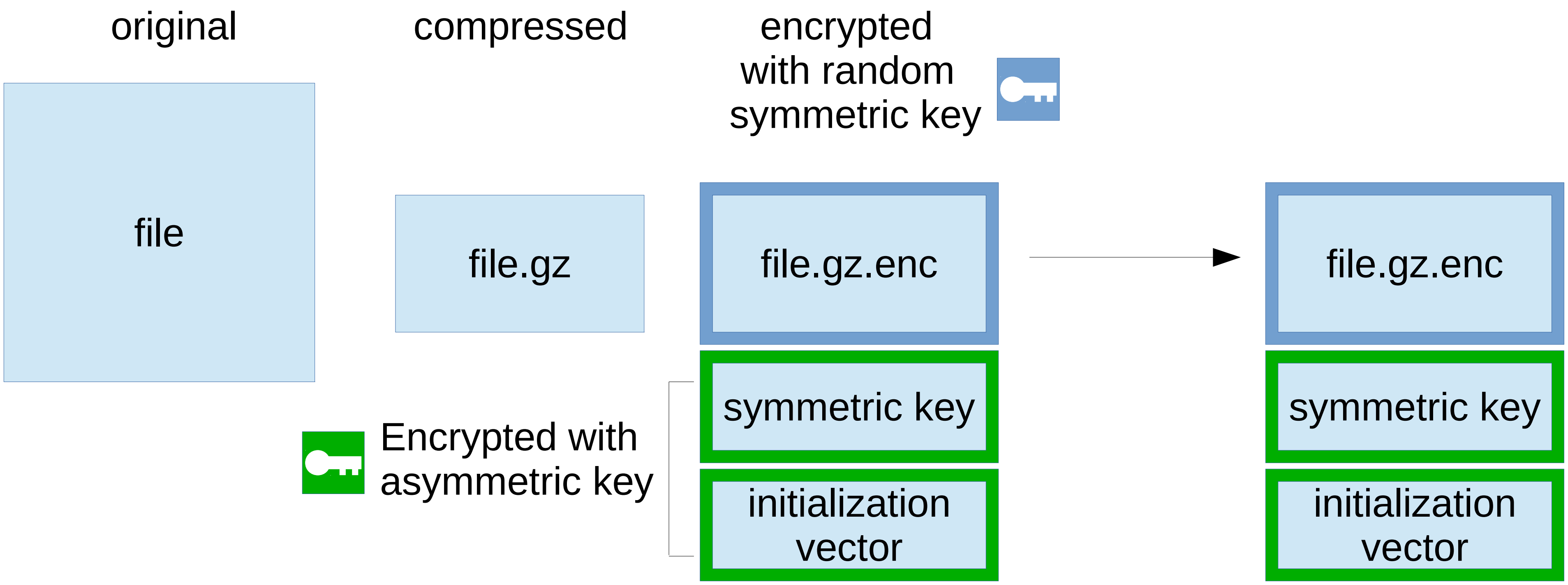
initialization vector

file.gz.enc

symmetric key

initialization vector

S3



original

compressed

encrypted
with random
symmetric key

file

file.gz

file.gz.enc

symmetric key

initialization vector

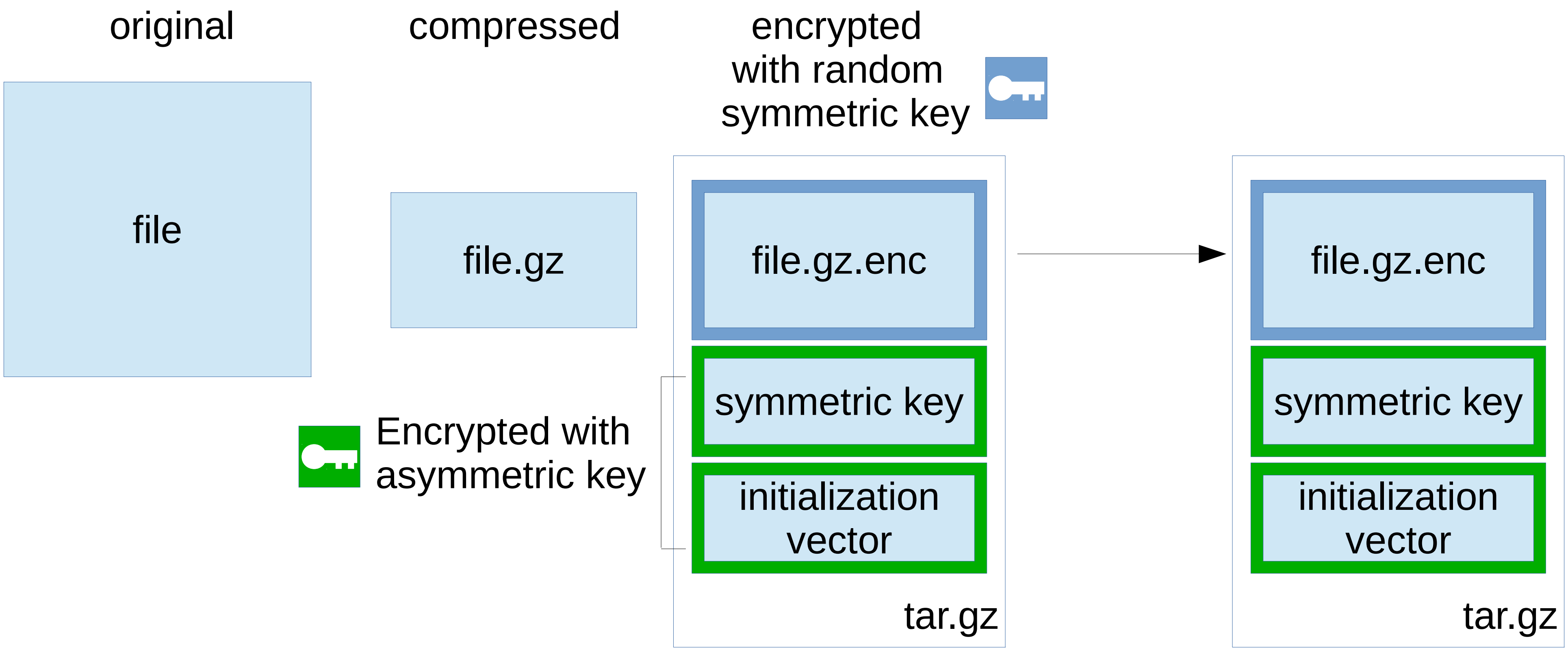
Encrypted with
asymmetric key

file.gz.enc

symmetric key

initialization vector

S3



original

compressed

encrypted with random symmetric key

file

file.gz

file.gz.enc

symmetric key

initialization vector

tar.gz

Encrypted with asymmetric key

file.gz.enc

symmetric key

initialization vector

tar.gz

connettiva.eu/rubyday2015

S3

OpenSSL::Cipher.new("aes-256-cbc")

OpenSSL::Pkey::RSA

SecureRandom.uuid

Digest::SHA256.hexdigest

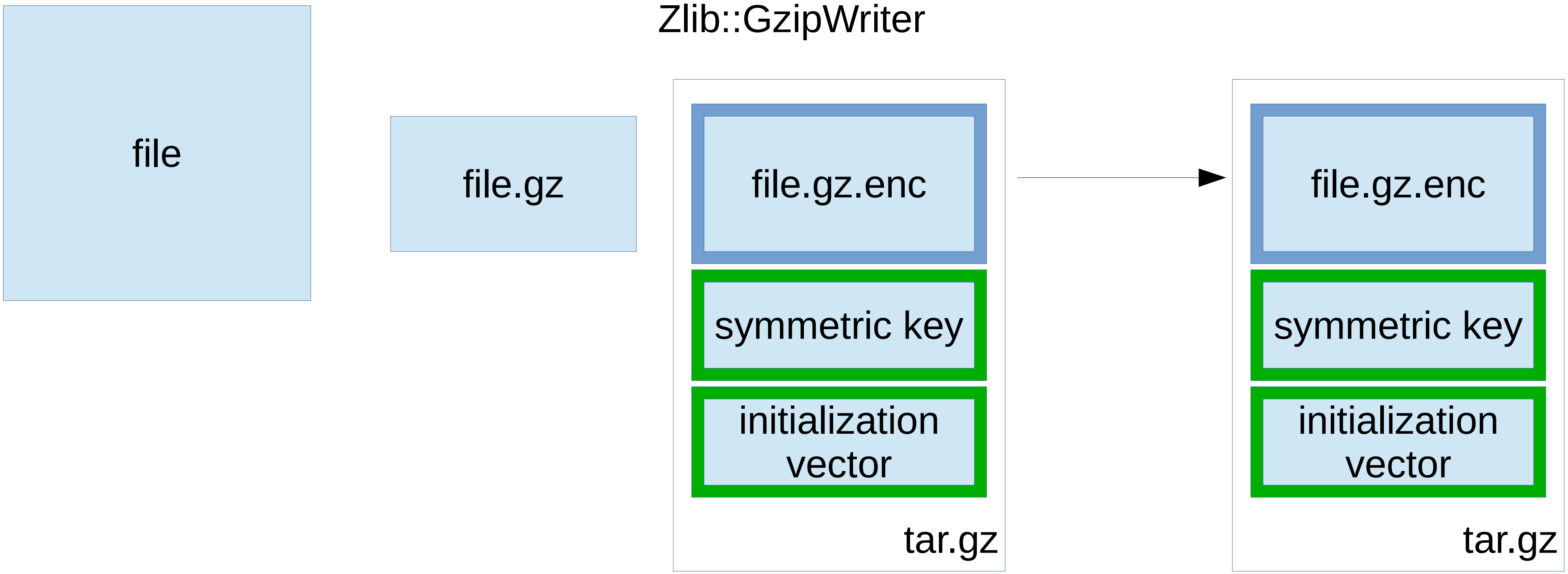
File.read("file")

Zlib::Deflate

Gem::Package::TarWriter

Aws::S3::Client

Zlib::GzipWriter



```
$ irb

require "openssl"

key = OpenSSL::PKey::RSA.new 4096

open 'private_key.pem', 'w' do |io|
  io.write key.to_pem
end

open 'public_key.pem', 'w' do |io|
  io.write key.public_key.to_pem
end
```

Using environmental variables to make it safe for production (Rails)

```
$ export PUBLIC_KEY=public_key.pem
$ export PRIVATE_KEY=private_key.pem
$ export BUCKET_NAME=your-amazon-bucket
```

```
# Gemfile or
$ gem install "aws-sdk" -v '~> 2'
$ irb
require "./safe_s3"
s3 = SafeS3.new
key = s3.upload("sensitive data")
 => "272ab006-c0be-4b79-97dd-8fb895af6d85...
s3.download(key)
 => "sensitive data"
s3.delete(key)
```

```
$ irb
require "./safe_s3"
s3 = SafeS3.new
key = s3.upload("sensitive data")
 => "272ab006-c0be-4b79-97dd-8fb895af6d85...
s3.download(key)
 => "sensitive data"
s3.delete(key)
```

connettiva.eu/rubyday2015