



# Security improvements in T<sub>E</sub>X Live

Norbert Preining

T<sub>E</sub>X Live Team

TUG 2016, Toronto

# Overview

- ▶ status up to (and including) 2015
- ▶ possible attack vectors
- ▶ integrity and authenticity
- ▶ verification architecture
- ▶ (non-)distributing GnuGP (and alternatives)
- ▶ Problems
- ▶ user experience
- ▶ key management

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font against a dark green background with a digital rain effect. The text is centered horizontally and occupies the lower half of the slide.

T<sub>E</sub>X Live 2016

## Status up to 2015

- ▶ container checksum (md5) is available in the tlpdb

---

```
name 12many
...
containersize 2100
containermd5 .....
doccontainersize 375404
doccontainermd5 ....
...
```

---

- ▶ but ...

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The background is a dark green field with a pattern of vertical lines and dots, resembling a digital rain or data stream effect.

T<sub>E</sub>X Live 2016

## Status up to 2015

- ▶ container checksum (md5) is available in the tlpdb

---

```
name 12many
...
containersize 2100
containermd5 .....
doccontainersize 375404
doccontainermd5 ....
...
```

---

- ▶ but ... only used to restart an interrupted installation

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital-style pattern that resembles a forest or a data visualization. The 'E' in 'T<sub>E</sub>X' has a subscript 'E' below it, and the '2016' is in a standard serif font.

## Status up to 2015

- ▶ container checksum (md5) is available in the tlpdb

---

```
name 12many
...
containersize 2100
containermd5 .....
doccontainersize 375404
doccontainermd5 ....
...
```

---

- ▶ but ... only used to restart an interrupted installation  
not for tlmgr update nor for normal installation!

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital-style pattern that resembles a forest or a data visualization. The 'E' in 'T<sub>E</sub>X' has a subscript 'E' below it, and the '2016' is in a standard serif font.

**Do we need better security?**



**T<sub>E</sub>X Live 2016**

## Possible attack vector I

- ▶ compromise one CTAN mirror

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered horizontally and set against a background of a green, pixelated, digital-style pattern that resembles a stylized 'matrix' or data stream. The letters are bold and clear, with the 'E' and 'X' having distinct subscripts.

T<sub>E</sub>X Live 2016

## Possible attack vector I

- ▶ compromise one CTAN mirror
- ▶ exchange pdftex binary with one shipping a crypto-virus

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font against a background of green, pixelated, vertical lines that resemble a digital rain or data stream effect.

T<sub>E</sub>X Live 2016



## Possible attack vector I

- ▶ compromise one CTAN mirror
- ▶ exchange pdftex binary with one shipping a crypto-virus
- ▶ enjoy ...

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital-style pattern that resembles a stylized forest or a data visualization. The 'E' in 'T<sub>E</sub>X' has a subscript 'E' below it, and the '2016' is in a standard serif font.

T<sub>E</sub>X Live 2016

## Possible attack vector I

- ▶ compromise one CTAN mirror
- ▶ exchange pdftex binary with one shipping a crypto-virus
- ▶ enjoy ...

Since no checks are done, this is easily possible!

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital rain effect, reminiscent of the Matrix movie. The 'E' in 'T<sub>E</sub>X' has a subscript 'E' below it, and the '2016' is in a standard serif font.

T<sub>E</sub>X Live 2016

## Possible attack vector I

- ▶ compromise one CTAN mirror
- ▶ exchange pdftex binary with one shipping a crypto-virus
- ▶ enjoy ...

Since no checks are done, this is easily possible!

Verification of checksums (md5)

In `tlcritical` for a few months before TL2016 was released, but not pushed out to 2015.

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, digital-style pattern that resembles a forest or a data stream, with vertical lines and a glowing effect.

T<sub>E</sub>X Live 2016

## Possible attack vectors II

- ▶ compromise one CTAN mirror

The logo for T<sub>E</sub>X Live 2016 is displayed in white text against a background of green digital rain. The text "T<sub>E</sub>X Live 2016" is centered and rendered in a large, bold, serif font. The background consists of vertical columns of green characters of varying heights and densities, creating a sense of data flow or a digital environment.

T<sub>E</sub>X Live 2016

## Possible attack vectors II

- ▶ compromise one CTAN mirror
- ▶ exchange pdftex binary with one shipping a crypto-virus

The logo for T<sub>E</sub>X Live 2016 is displayed against a background of green digital rain. The text "T<sub>E</sub>X Live 2016" is rendered in a white, serif font, with the "E" in "T<sub>E</sub>X" being significantly larger and more prominent than the other letters.

T<sub>E</sub>X Live 2016

## Possible attack vectors II

- ▶ compromise one CTAN mirror
- ▶ exchange pdftex binary with one shipping a crypto-virus
- ▶ adjust the container that the MD5 sum does not change (possible!)

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font against a background of green, pixelated, vertical lines that resemble a digital rain or data stream effect.

T<sub>E</sub>X Live 2016

## Possible attack vectors II

- ▶ compromise one CTAN mirror
- ▶ exchange pdftex binary with one shipping a crypto-virus
- ▶ adjust the container that the MD5 sum does not change (possible!)
- ▶ enjoy ...

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital rain effect, reminiscent of the Matrix movie. The 'E' in 'T<sub>E</sub>X' has a subscript 'E' below it.

T<sub>E</sub>X Live 2016

## Possible attack vectors II

- ▶ compromise one CTAN mirror
- ▶ exchange pdftex binary with one shipping a crypto-virus
- ▶ adjust the container that the MD5 sum does not change (possible!)
- ▶ enjoy ...

No counter measures up to T<sub>E</sub>X Live 2015!

The logo for T<sub>E</sub>X Live 2016 features the text "T<sub>E</sub>X Live 2016" in a large, white, serif font. The text is centered against a background of a dense, green, pixelated pattern that resembles a digital rain or data stream, similar to the aesthetic of the movie The Matrix.



## Possible attack vector III

- ▶ compromise one CTAN mirror (or setup one yourself, get good connections and many users)

The logo for T<sub>E</sub>X Live 2016 is displayed against a background of a green digital rain effect, similar to the Matrix movie. The text "T<sub>E</sub>X Live 2016" is written in a white, serif font. The 'E' in "T<sub>E</sub>X" has a subscript 'E' below it. The 'L' in "Live" is a simple capital letter. The '2016' is in a standard serif font.

T<sub>E</sub>X Live 2016

## Possible attack vector III

- ▶ compromise one CTAN mirror (or setup one yourself, get good connections and many users)
- ▶ exchange pdftex binary as before

The logo for T<sub>E</sub>X Live 2016 is displayed against a background of green digital rain. The text "T<sub>E</sub>X Live 2016" is rendered in a white, serif font, with the "E" in "T<sub>E</sub>X" having a subscript "E" below it.

T<sub>E</sub>X Live 2016

## Possible attack vector III

- ▶ compromise one CTAN mirror (or setup one yourself, get good connections and many users)
- ▶ exchange pdftex binary as before
- ▶ adjust the checksum in the t<sub>l</sub>pdb file

The logo for T<sub>E</sub>X Live 2016 is displayed in white text against a background of green, pixelated, vertical lines that resemble a digital rain or data stream effect.

T<sub>E</sub>X Live 2016

## Possible attack vector III

- ▶ compromise one CTAN mirror (or setup one yourself, get good connections and many users)
- ▶ exchange pdftex binary as before
- ▶ adjust the checksum in the t<sub>l</sub>pdb file
- ▶ enjoy ...

The logo for T<sub>E</sub>X Live 2016 is displayed in white, bold, sans-serif font against a background of green, pixelated, vertical lines that resemble a digital rain or data stream effect.

T<sub>E</sub>X Live 2016

## Possible attack vector III

- ▶ compromise one CTAN mirror (or setup one yourself, get good connections and many users)
- ▶ exchange pdftex binary as before
- ▶ adjust the checksum in the t<sub>l</sub>pdb file
- ▶ enjoy ...

No counter measures up to T<sub>E</sub>X Live 2015!

The logo for T<sub>E</sub>X Live 2016 is displayed in large, white, serif font against a background of green, pixelated, digital-style patterns. The text "T<sub>E</sub>X Live 2016" is centered horizontally and vertically within the lower half of the slide.

T<sub>E</sub>X Live 2016

# Integrity and authenticity



**T<sub>E</sub>X Live 2016**

# Integrity and authenticity

## Integrity

Need to check the integrity of the downloaded packages – prevent tampering.

The logo for T<sub>E</sub>X Live 2016 is displayed in white text against a dark green background with a digital rain effect. The text is arranged in two lines: "T<sub>E</sub>X Live" on the top line and "2016" on the bottom line.

T<sub>E</sub>X Live 2016

# Integrity and authenticity

## Integrity

Need to check the integrity of the downloaded packages – prevent tampering.

MD5 is not strong, can be tampered

The logo for T<sub>E</sub>X Live 2016 is displayed in white, bold, serif font against a background of green, pixelated, vertical lines that resemble a digital or matrix-style aesthetic.

T<sub>E</sub>X Live 2016



# Integrity and authenticity

## Integrity

Need to check the integrity of the downloaded packages – prevent tampering.

MD5 is not strong, can be tampered – switch to SHA512

The logo for T<sub>E</sub>X Live 2016 is displayed in white, bold, sans-serif font against a dark green background. The background features a vertical stream of green characters, resembling a digital rain or data stream, which is a common visual motif for the T<sub>E</sub>X Live project.

T<sub>E</sub>X Live 2016

# Integrity and authenticity

## Integrity

Need to check the integrity of the downloaded packages – prevent tampering.

MD5 is not strong, can be tampered – switch to SHA512

## Authenticity

Verify that the packages are actually the ones from us (T<sub>E</sub>X Live Team).

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital rain effect, reminiscent of the Matrix movie. The letters are bold and clear, with the 'E' in 'T<sub>E</sub>X' having a subscript 'E' and the '2016' being in a standard font weight.

T<sub>E</sub>X Live 2016

# Integrity and authenticity

## Integrity

Need to check the integrity of the downloaded packages – prevent tampering.

MD5 is not strong, can be tampered – switch to SHA512

## Authenticity

Verify that the packages are actually the ones from us (T<sub>E</sub>X Live Team).

Cryptographic signatures

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The background is a dark green field with a pattern of vertical lines and dots, resembling a digital or matrix-style aesthetic.

T<sub>E</sub>X Live 2016

## Verification architecture - overview



T<sub>E</sub>X Live 2016

## Verification architecture - overview

```
tlmgr downloads remote texlive.tlpdb
```

The logo for T<sub>E</sub>X Live 2016 is displayed against a background of a green digital rain effect, similar to the Matrix movie. The text "T<sub>E</sub>X Live 2016" is written in a large, white, serif font.

T<sub>E</sub>X Live 2016

## Verification architecture - overview

t<sub>l</sub>mgr downloads remote texlive.t<sub>l</sub>pdb

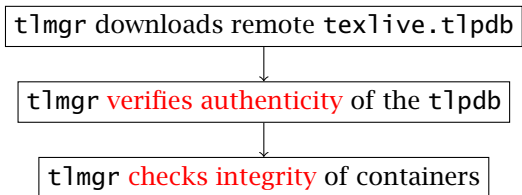


t<sub>l</sub>mgr **verifies authenticity** of the t<sub>l</sub>pdb



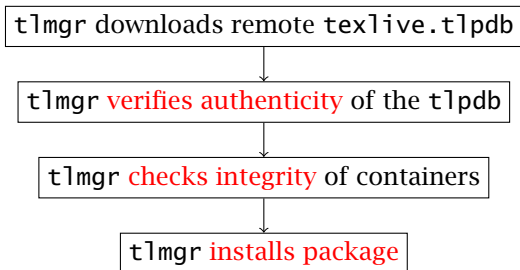
# T<sub>E</sub>X Live 2016

## Verification architecture - overview



T<sub>E</sub>X Live 2016

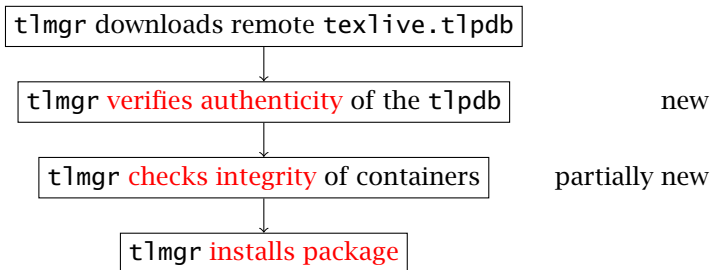
## Verification architecture - overview



# T<sub>E</sub>X Live 2016



## Verification architecture - overview



# T<sub>E</sub>X Live 2016

## Verification of authenticity



**T<sub>E</sub>X Live 2016**

## Verification of authenticity

*texlive.tlpdb*

```
name 00texlive.config
...

name 12many
containerchecksum ...
...

name 2up
containerchecksum ...
...
```

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is set against a background of a green, pixelated, digital-style pattern that resembles a stylized 'matrix' or 'data stream' effect. The letters are bold and clearly legible.

**T<sub>E</sub>X Live 2016**

## Verification of authenticity

*texlive.tlpdb*

```
name 00texlive.config
...

name 12many
containerchecksum ...
...

name 2up
containerchecksum ...
...
```

→

*texlive.tlpdb.sha512*

```
<128 hex digits> texlive.tlpdb
```

**T<sub>E</sub>X Live 2016**

## Verification of authenticity

*texlive.tlpdb*

```
name 00texlive.config
...

name 12many
containerchecksum ...
...

name 2up
containerchecksum ...
...
```

→

*texlive.tlpdb.sha512*

```
<128 hex digits> texlive.tlpdb
```

↓

*texlive.tlpdb.sha512.asc*

```
--BEGIN PGP SIGNATURE--

iQEVAwUBVyAV9kzhh3...
r2mB9xEnR4o2SRBDNI...
...
--END PGP SIGNATURE--
```

# TeX Live 2016

## Signing key

---

```
pub 2048R/06BAB6BC 2016-03-19
   Key fingerprint = C78B 82D8 C795 12F7 9CC0 D7C8 0D5E 5D91 06BA B6BC
uid      TeX Live Distribution <tex-live@tug.org>
sig 3 06BAB6BC 2016-03-19 TeX Live Distribution <tex-live@tug.org>
sig 3 06BAB6BC 2016-03-19 TeX Live Distribution <tex-live@tug.org>
sig 860CDC13 2016-03-20 Norbert Preining <norbert@preining.info>
sig 30D155AD 2016-03-20 Karl Berry <karl@freefriends.org>
```

---

- ▶ signed by Karl and my key (mine is also in the Debian keyring)
- ▶ actual signing subkey is used, main key is offline  
(in case of breach of TUG server we can revoke the sub-key)



The logo for TeX Live 2016 features the text 'T<sub>E</sub>X Live 2016' in a white, serif font. The text is set against a dark background with a vibrant green, pixelated or digital rain effect, reminiscent of the Matrix movie. The 'E' in 'T<sub>E</sub>X' has a subscript 'E'.

## Verification of authenticity II

Why not sign directly?



T<sub>E</sub>X Live 2016

## Verification of authenticity II

Why not sign directly?

- ▶ speed up of verification (factor 10)

The logo for T<sub>E</sub>X Live 2016 is displayed in white text against a background of green, pixelated, vertical lines that resemble a digital rain or data stream effect.

T<sub>E</sub>X Live 2016



## Verification of authenticity II

### Why not sign directly?

- ▶ speed up of verification (factor 10)
- ▶ (because this is how I copied it from Debian)

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital-style pattern that resembles a forest or a data visualization. The 'E' in 'T<sub>E</sub>X' has a subscript 'E' below it.

T<sub>E</sub>X Live 2016

## Verification of authenticity II

### Why not sign directly?

- ▶ speed up of verification (factor 10)
- ▶ (because this is how I copied it from Debian) might not be needed (0.01s versus 0.1s)?

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The background is a dark green field with a pattern of vertical lines and dots, resembling a digital or matrix-style aesthetic.

T<sub>E</sub>X Live 2016

## Verification of authenticity II

### Why not sign directly?

- ▶ speed up of verification (factor 10)
- ▶ (because this is how I copied it from Debian) might not be needed (0.01s versus 0.1s)?

### Why SHA512?

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital rain effect, reminiscent of the Matrix movie. The 'E' in 'T<sub>E</sub>X' has a subscript 'E' below it, and the '2016' is in a standard serif font.

T<sub>E</sub>X Live 2016

## Verification of authenticity II

### Why not sign directly?

- ▶ speed up of verification (factor 10)
- ▶ (because this is how I copied it from Debian) might not be needed (0.01s versus 0.1s)?

### Why SHA512?

- ▶ currently considered uncompromisable (in contrast to MD5)
- ▶ will hopefully hold for several years (other options SHA256 etc)

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font against a background of a green, pixelated, digital rain effect. The text "T<sub>E</sub>X Live 2016" is centered horizontally and occupies the lower half of the slide.

T<sub>E</sub>X Live 2016

## Check of integrity

Check the SHA512 checksum of the containers against the (verified) information in the `texlive.tlpdb`.

The logo for T<sub>E</sub>X Live 2016 is displayed against a background of a green digital rain effect, similar to the Matrix movie. The text "T<sub>E</sub>X Live 2016" is written in a white, serif font. The 'E' in "T<sub>E</sub>X" has a subscript 'E' below it. The 'L' in "Live" is a simple capital letter. The '2016' is in a large, bold, sans-serif font.

T<sub>E</sub>X Live 2016

## Check of integrity

Check the SHA512 checksum of the containers against the (verified) information in the `texlive.tlpdb`.

### Comments

- ▶ Why sufficient?

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The background is a dark green field filled with vertical columns of bright green, pixelated characters, resembling a digital rain or data stream effect.

T<sub>E</sub>X Live 2016

## Check of integrity

Check the SHA512 checksum of the containers against the (verified) information in the `texlive.tlpdb`.

### Comments

- ▶ Why sufficient? — `texlive.tlpdb` gives authenticated information

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The background is a dark green field with a pattern of vertical lines and dots, resembling a digital rain or matrix effect.

T<sub>E</sub>X Live 2016

## Check of integrity

Check the SHA512 checksum of the containers against the (verified) information in the `texlive.tlpdb`.

### Comments

- ▶ Why sufficient? — `texlive.tlpdb` gives authenticated information
- ▶ We actually check also the size (might delete that one!)

The logo for T<sub>E</sub>X Live 2016 is displayed in white, bold, sans-serif font against a background of a green, pixelated, digital rain effect. The text is arranged in two lines: "T<sub>E</sub>X Live" on the top line and "2016" on the bottom line.

T<sub>E</sub>X Live 2016



## (Non-)distributing of GnuPG

Why not include GnuPG into T<sub>E</sub>X Live?

The logo for T<sub>E</sub>X Live 2016 features the text "T<sub>E</sub>X Live 2016" in a white, serif font. The background is a dark green field with a pattern of vertical lines and dots, resembling a digital or matrix-style aesthetic.

T<sub>E</sub>X Live 2016

## (Non-)distributing of GnuPG

Why not include GnuPG into T<sub>E</sub>X Live?

- ▶ We don't want to support (and compile it)

The logo for T<sub>E</sub>X Live 2016 is displayed against a background of a green digital rain effect. The text "T<sub>E</sub>X Live 2016" is written in a large, white, serif font. The 'E' in "T<sub>E</sub>X" has a subscript 'E' below it. The 'L' in "Live" is also large and white. The "2016" is in a smaller white font to the right of "Live".

T<sub>E</sub>X Live 2016

## (Non-)distributing of GnuPG

Why not include GnuPG into T<sub>E</sub>X Live?

- ▶ We don't want to support (and compile it)  
(but could go into private space like xz and wget!)

The logo for T<sub>E</sub>X Live 2016 features the text "T<sub>E</sub>X Live 2016" in a white, serif font. The text is centered and overlaid on a background of a green, pixelated, digital rain effect, reminiscent of the Matrix movie. The background is dark with bright green vertical streaks and dots.

T<sub>E</sub>X Live 2016

## (Non-)distributing of GnuPG

Why not include GnuPG into T<sub>E</sub>X Live?

- ▶ We don't want to support (and compile it)  
(but could go into private space like xz and wget!)
- ▶ Export and import restrictions, Waasenaar Agreement  
Export might be ok nowadays, but there are many countries the strictly forbid *import* of cryptographic software (India, France is a bit unclear, ...)  
TUG does not want to get involved in legal battles (not funny) when sending DVDs to India or other countries.

The logo for T<sub>E</sub>X Live 2016 is displayed against a background of a green digital rain effect, similar to the Matrix movie. The text "T<sub>E</sub>X Live 2016" is written in a large, white, serif font. The 'E' in "T<sub>E</sub>X" has a subscript 'E' below it. The 'L' in "Live" is also in a serif font. The year "2016" is in a similar serif font.

T<sub>E</sub>X Live 2016

## Alternative for T<sub>E</sub>X Live

```
tlmgr -repository http://www.preining.info/tlgpg/  
install tlgpg
```

The logo for T<sub>E</sub>X Live 2016 features the text "T<sub>E</sub>X Live 2016" in a white, serif font. The text is centered against a background of a green, pixelated, digital rain effect, reminiscent of the Matrix movie. The letters are large and bold, with the 'E' and 'X' having a distinct subscripted 'E' and 'X' respectively.

T<sub>E</sub>X Live 2016

## Alternative for T<sub>E</sub>X Live

```
tlmgr -repository http://www.preining.info/tlpgg/  
install tlpgg
```

- ▶ installs binaries into `tlpkg/installer/gpg/`
- ▶ GnuPG binaries for Windows and Mac (both archs)
- ▶ already supported by TLU on Mac
- ▶ most big distributions have GnuPG (1 or 2) installed (both fine)
- ▶ the T<sub>E</sub>X Live infrastructure already checks for the above location
- ▶ not affiliated with TUG (smile)
- ▶ maybe could be hosted at DANTE or some other server?

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital-style pattern that resembles a stylized 'matrix' or 'data stream' effect. The letters are bold and clear, with the 'E' and 'X' having distinct horizontal bars.

T<sub>E</sub>X Live 2016

# Problems



**T<sub>E</sub>X Live 2016**

# Problems

## Computing SHA512 checksums

- ▶ we use `Digest::SHA` perl module

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The background is a dark green field with a pattern of vertical lines and dots, resembling a digital or matrix aesthetic. The text is centered horizontally and occupies the lower half of the slide.

T<sub>E</sub>X Live 2016



# Problems

## Computing SHA512 checksums

- ▶ we use `Digest::SHA` perl module, but this is not available on older MacOS (shipping 10 years old Perl!)

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered horizontally and set against a dark green background that features a vertical stream of glowing green dots, resembling a digital rain or data stream effect.

T<sub>E</sub>X Live 2016

# Problems

## Computing SHA512 checksums

- ▶ we use `Digest::SHA` perl module, but this is not available on older MacOS (shipping 10 years old Perl!)
- ▶ Perl/Lua implementation is **far** too slow (minutes!)

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font against a dark green background with a digital, matrix-like pattern of glowing green dots and lines.

T<sub>E</sub>X Live 2016

# Problems

## Computing SHA512 checksums

- ▶ we use `Digest::SHA` perl module, but this is not available on older MacOS (shipping 10 years old Perl!)
- ▶ Perl/Lua implementation is **far** too slow (minutes!)
- ▶ Solution: try `Digest::SHA`, `openssl`, `sha512sum`, and `shasum`, one is hopefully available

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital-style pattern that resembles a stylized 'matrix' or 'data stream' effect. The letters are bold and clear, with the 'E' and 'X' having distinct subscripts.

T<sub>E</sub>X Live 2016

# Problems

## Computing SHA512 checksums

- ▶ we use `Digest::SHA` perl module, but this is not available on older MacOS (shipping 10 years old Perl!)
- ▶ Perl/Lua implementation is **far** too slow (minutes!)
- ▶ Solution: try `Digest::SHA`, `openssl`, `sha512sum`, and `shasum`, one is hopefully available

## Users' complains

reduce visibility of warnings/information shown,  
try to provide a unspectacular introduction of the feature

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital-style pattern that resembles a stylized 'matrix' or 'data stream' effect. The letters are bold and clear, with the 'E' in 'T<sub>E</sub>X' having a subscript 'E'.

# User experience – changes in the interface

Aim: nearly no user visible change

The bottom of the slide features a decorative background of green digital rain. Overlaid on this background is the text "T<sub>E</sub>X Live 2016" in a large, white, serif font.

T<sub>E</sub>X Live 2016

## User experience – changes in the interface

Aim: nearly no user visible change

---

```
[~] tlmgr update --list --repository http://localhost/tlnet/  
tlmgr: package repository http://localhost/tlnet/ (verified)  
...
```

---

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The background is a dark green field with a pattern of vertical, glowing green lines, resembling a digital rain or data stream effect.

T<sub>E</sub>X Live 2016

## User experience – changes in the interface

Aim: nearly no user visible change

---

```
[~] tlmgr update --list --repository http://localhost/tlnet/  
tlmgr: package repository http://localhost/tlnet/ (verified)  
...
```

---

If not GnuPG is found the output is:

---

```
[~] tlmgr update --list --repository http://localhost/tlnet/  
tlmgr: package repository http://localhost/tlnet/ (not verified)  
...
```

---

Similar for multiple repositories

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital rain effect, reminiscent of the Matrix movie. The 'E' in 'T<sub>E</sub>X' has a subscript 'E' below it, and the '2016' is in a standard serif font.

# Key management

Aim: support alternative repositories

- ▶ `t1mgr` key action added
- ▶ allows listing, adding, removing of keys
- ▶ already in use (koma script, TeX JP, ...)

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font against a background of green, pixelated, vertical lines that resemble a digital rain or data stream effect.

T<sub>E</sub>X Live 2016



## Further plans

not many ...



**T<sub>E</sub>X Live 2016**

## Further plans

not many ...

- ▶ download checksum from TUG for extra protection?
- ▶ directly sign - reduce one download?
- ▶ do not check file size (useless overhead)?

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital rain effect, reminiscent of the Matrix movie. The 'E' in 'T<sub>E</sub>X' has a subscript 'E' below it, and the '2016' is in a standard serif font.

T<sub>E</sub>X Live 2016

## Further plans

not many ...

- ▶ download checksum from TUG for extra protection?
- ▶ directly sign - reduce one download?
- ▶ do not check file size (useless overhead)?
- ▶ ... your suggestions?

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital-style pattern that resembles a forest or a data visualization. The 'E' in 'T<sub>E</sub>X' has a subscript 'E' below it, and the '2016' is in a standard serif font.

T<sub>E</sub>X Live 2016

## Further plans

not many ...

- ▶ download checksum from TUG for extra protection?
- ▶ directly sign - reduce one download?
- ▶ do not check file size (useless overhead)?
- ▶ ... your suggestions?

Thanks for your attention

The logo for T<sub>E</sub>X Live 2016 is displayed in a large, white, serif font. The text is centered against a background of a green, pixelated, digital rain effect, reminiscent of the Matrix movie. The 'E' in 'T<sub>E</sub>X' has a subscript 'E' below it, and the '2016' is in a standard serif font.

T<sub>E</sub>X Live 2016