Web of Trust for distribution keyrings

Distributing trust for Arch Linux

David Runge

2022-12-29

Who?

- Arch Linux Package Maintainer (2017)/ Developer (2019)
- Main signing key since 2021
- Maintaining keyringctl[1]

[1] https://gitlab.archlinux.org/archlinux/keyringctl

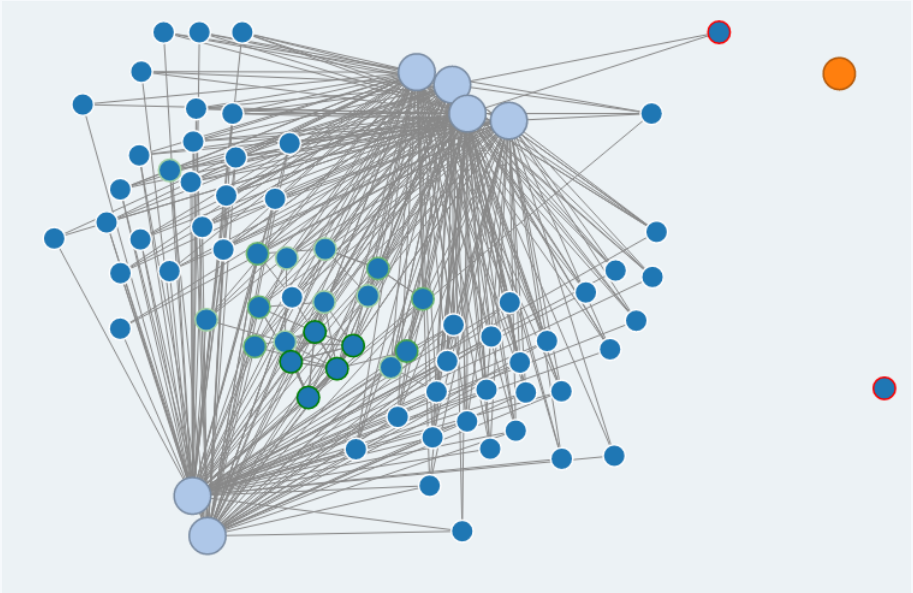
Web of Trust (WoT)

- Web of Trust for packager keys
- Packager keys are signed by main signing keys
- Packagers can only push packages, if their keys have at least three signatures

Main signing keys

Master Key	Full Fingerprint	Owner	Owner's Signing Key	Revoker	Revoker's Signing Key	Developer/TU Keys Signed
0x6AC6A4C2	0E8B 6440 79F5 99DF C1DD C397 3348 882F 6AC6 A4C2	Pierre Schmitz	0x54449A5C	Ronald van Haren	0x8406FFF3	71
0x77514E00	91FF E070 0E80 619C EB73 235C A88E 23E3 7751 4E00	Florian Pritz	0x4CE1C13E	Lukas Fleischer	0x9326B440	78
0x27843F1C	D8AF DDA0 7A5B 6EDF A7D8 CCDA D6D0 55F9 2784 3F1C	Levente Polyak	0x8D8172C8	Evangelos Foutras	0xA9999C34	50
0x7BE9892E	2AC0 A42E FB0B 5CBC 7A04 02ED 4DC9 5B6D 7BE9 892E	David Runge	0x5BF0D338	Christian Hesse	0x498E9CEE	70
0xCC52A02A	75BD 80E4 D834 509F 6E74 0257 B1B7 3B02 CC52 A02A	Jonas Witschel	0x46879D04	Frederik Schwan	0x5426DA0A	62
0x037F4F41	69E6 471E 3AE0 6529 7529 832E 6BA0 F5A2 037F 4F41	Johannes Löthberg	0x3A9D0BB5	Maxime Gauduin	0x81506130	49

Key cloud



Signature example

```
❯ pacman-key --list-sigs 991F6E3F0765CF62958858613 9B09DA5BF0D338
gpg: Note: trustdb not writable
pub   ed25519 2022-05-10 [SC] [expires: 2026-05-09]
      991F6E3F0765CF62958858613 9B09DA5BF0D338
uid           [  full  ] David Runge <dvzrv@archlinux.org>
sig 3        139B09DA5BF0D338 2022-05-10  David Runge <dvzrv@archlinux.org>
sig          B1B73B02CC52A02A 2022-07-09  Jonas Witschel (Arch Linux Master Key) <diabonas@master-key.archlinux.org>
sig          A88E23E377514E00 2022-06-05  Florian Pritz (Arch Linux Master Key) <florian@master-key.archlinux.org>
sig          4DC95B6D7BE9892E 2022-05-19  David Runge (Arch Linux Master Key) <dvzrv@master-key.archlinux.org>
sig 3        7258734B41C31549 2022-05-10  David Runge <dvzrv@archlinux.org>
sig          D6D055F927843F1C 2022-08-02  Levente Polyak (Arch Linux Master Key) <anthraxx@master-key.archlinux.org>
sig          6BA0F5A2037F4F41 2022-11-29  Johannes Löthberg (Arch Linux Master Key) <demize@master-key.archlinux.org>
sub   ed25519 2022-05-10 [A] [expires: 2026-05-09]
sig          139B09DA5BF0D338 2022-05-10  David Runge <dvzrv@archlinux.org>
sub   cv25519 2022-05-10 [E] [expires: 2026-05-09]
sig          139B09DA5BF0D338 2022-05-10  David Runge <dvzrv@archlinux.org>
```

Web of Trust on each target host

- WoT using a system-wide gnupg keyring
- Locally unique system key lsigns main signing keys
- Importing of updated/new keys as alpm-hook[2]
- Hopefully soon also flat-file support[3] as using WoT on the target is flaky

[2] https://man.archlinux.org/man/core/pacman/alpm-hooks.5.en
[3] https://gitlab.archlinux.org/archlinux/keyringctl/-/issues/3

Maintaining a curated keyring

- Used to be a bash script pulling from SKS[4]
- SKS is dead and keyservers are *weird* (WKD is *also weird*)
- Keyringctl to the rescue!

[4] https://github.com/SKS-Keyserver/sks-keyserver

Keyringctl

- Using sequoia-sq[5]
- Decomposed directory structure
- Operating on OpenPGP packet level
- Keys and signatures are added and updated by adding them to a git repository
- Export to WKD[6]

[5] https://sequoia-pgp.org/
[6] https://wiki.gnupg.org/WKD

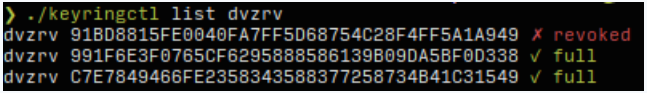
Archlinux-keyring packager key example

```
❯ tree keyring/packager/dvzrv/991F6E3F0765CF6295888586139B09DA5BF0D338
keyring/packager/dvzrv/991F6E3F0765CF6295888586139B09DA5BF0D338
├── 991F6E3F0765CF6295888586139B09DA5BF0D338.asc
├── subkey
│   ├── 5F1EB5EA50E5936FA97BCF484B25DE8BCC520558
│   │   ├── 5F1EB5EA50E5936FA97BCF484B25DE8BCC520558.asc
│   │   └── certification
│   │       └── 991F6E3F0765CF6295888586139B09DA5BF0D338.asc
│   └── 84471F40DFE31E5763BAFF2DBCA1AA1BD6B976F5
│       ├── 84471F40DFE31E5763BAFF2DBCA1AA1BD6B976F5.asc
│       └── certification
│           └── 991F6E3F0765CF6295888586139B09DA5BF0D338.asc
└── uid
    └── David_Runge__dvzrv@archlinux.org_d2ad250f
        ├── David_Runge__dvzrv@archlinux.org_d2ad250f.asc
        └── certification
            ├── 2AC0A42EFB0B5CBC7A0402ED4DC95B6D7BE9892E.asc
            ├── 69E6471E3AE065297529832E6BA0F5A2037F4F41.asc
            ├── 75BD80E4D834509F6E740257B1B73B02CC52A02A.asc
            ├── 91FFE0700E80619CEB73235CA88E23E377514E00.asc
            ├── 991F6E3F0765CF6295888586139B09DA5BF0D338.asc
            ├── C7E7849466FE2358343588377258734B41C31549.asc
            └── D8AFDDA07A5B6EDFA7D8CCDAD6D055F927843F1C.asc

9 directories, 13 files
```

Keyringctl inspect

```
❯ ./keyringctl inspect 991F6E3F0765CF62958888586139B09DA5BF0D338

WARNING: sq does not have a stable CLI interface.  Use with caution in scripts.

/run/user/1000/arch-keyringctl-6urqvadp/packet-_ztngwsb.asc: OpenPGP Certificate.

    Fingerprint: 991F6E3F0765CF62958888586139B09DA5BF0D338 dvzrv ✓ full
Public-key algo: EdDSA
Public-key size: 256 bits
  Creation time: 2022-05-10 08:21:58 UTC
Expiration time: 2026-05-09 08:21:58 UTC (creation time + P1460D)
      Key flags: certification, signing

         Subkey: 84471F40DFE31E5763BAFF2DBCA1AA1BD6B976F5
Public-key algo: EdDSA
Public-key size: 256 bits
  Creation time: 2022-05-10 08:25:24 UTC
Expiration time: 2026-05-09 08:25:24 UTC (creation time + P1460D)
      Key flags: authentication

         Subkey: 5F1EB5EA50E5936FA97BCF484B25DE8BCC520558
Public-key algo: ECDH
Public-key size: 256 bits
  Creation time: 2022-05-10 08:21:58 UTC
Expiration time: 2026-05-09 08:21:58 UTC (creation time + P1460D)
      Key flags: transport encryption, data-at-rest encryption

         UserID: David Runge <dvzrv@archlinux.org>
  Certification: Creation time: 2022-11-29 21:36:34 UTC
                 Alleged certifier: 69E6471E3AE065297529832E6BA0F5A2037F4F41 demize (main) ✓ full
                 Hash algorithm: SHA512
  Certification: Creation time: 2022-08-02 17:04:04 UTC
                 Alleged certifier: D8AFDDA07A5B6EDFA7D8CCDAD6D055F927843F1C anthraxx (main) ✓ full
                 Hash algorithm: SHA512
  Certification: Creation time: 2022-07-09 08:56:55 UTC
                 Alleged certifier: 75BD80E4D834509F6E740257B1B73B02CC52A02A diabonas (main) ✓ full
                 Hash algorithm: SHA512
  Certification: Creation time: 2022-06-05 12:48:00 UTC
                 Alleged certifier: 91FFE0700E80619CEB73235CA88E23E377514E00 florian (main) ✓ full
                 Hash algorithm: SHA512
  Certification: Creation time: 2022-05-19 23:11:33 UTC
                 Alleged certifier: 2AC0A42EFB0B5CBC7A0402ED4DC95B6D7BE9892E dvzrv (main) ✓ full
                 Hash algorithm: SHA512
  Certification: Creation time: 2022-05-10 09:45:07 UTC
                 Alleged certifier: C7E7849466FE2358343588377258734B41C31549 dvzrv ✓ full
                 Hash algorithm: SHA512
           Note: Certifications have NOT been verified!
```

Keyringctl list



Keyringctl list revoked

```
× 130 ❯ ./keyringctl list --trust revoked
aginiewicz     717026A9D4779FC53940726640F557B731496106 ✗ revoked
alad           DBE7D3DD8C81D58D0A13D0E76BC26A17B9B7018A ✗ revoked
alucryd        9437DD3815A7A9169E3D3946AFF5D95098BC6FF5 ✗ revoked
ambrevar       50F33E2E5B0C3D900424ABE89BDCF497A4BBCC7F ✗ revoked
andrea         4FCF887689C41B09506BE8D5F3E1D5C5D30DB0AD ✗ revoked
angvp          40776A5221EF5AD468A4906D42A1DB15EC133BAD ✗ revoked
arcanis        779CD2942629B7FA04AB8F172E89012331361F01 ✗ revoked
bisson         1A60DC44245D06FEF90623D6EEEEE2EEEE2EEEEE ✗ revoked
bisson         5A2257D19FF7E1E0E415968CE62F853100F0D0F0 ✗ revoked
bpiotrowski    F3691687D867B81B51CE07D9BBE43771487328A9 ✗ revoked
```

Keyringctl list marginal

```
❯ ./keyringctl list --trust marginal
arodseth      962855F072C7A01846405864FCF3C8CB5CF9C8D4 ~ marginal
cbehan        6EA3F3F3B9082632A9CBE931D53A0445B47A0DAB ~ marginal
dbermond      3FFA6AB7B69AAE6CCA263DDE019A7474297D8577 ~ marginal
djgera        0F334D8698881578F65D2AE55ED514A45BD5C938 ~ marginal
escondida     CB33B736591A9CA06098A9A5FCAC9CF5A6EE1209 ~ marginal
farseerfc     4B1DE545A801D4549BFD3FEF90CB3D62C13D4796 ~ marginal
ibiru         F4DDD6DDCEC320B665F502AAE8F18BA1615137BC ~ marginal
juergen       355BDB97ED4724E6B3A450E7A3D9562A589874AB ~ marginal
kgizdov       4BE61D684CB4E31741614E7089AA27231C530226 ~ marginal
kkeen         48C3B1F30DDD0FE67E516D16396E3E25BAB142C1 ~ marginal
maximbaz      EB4F9E5A60D32232BB52150C12C87A28FEAC6B20 ~ marginal
mtorromeo     2C118C620F02DB9AC1D0F9FA94DD2393DA2EE423 ~ marginal
muflone       C521846436D75A3294795B27B4360204B250F0D3 ~ marginal
spupykin      3E518BF2526FD1979E8AAE4965C110C1EA433FC7 ~ marginal
tensor5       A9B6710D760F6617C530746EC847B6AEB0544167 ~ marginal
wild          0E87D6C3F9AF7FDED0C8588D22E3B67B4A86FDE7 ~ marginal
xyne          EC3CBE7F607D11E663149E811D1F0DC78F173680 ~ marginal
```

Contact

David Runge

Mail: dave@sleepmap.de

Matrix: @dvzrv:matrix.org

IRC: dvzrv@{hackint,libera,oftc}