



Package Signing with Post-Quantum Cryptography



Zach Steindler
Principal Security Engineer
GitHub / npm

Agenda

- How are npm packages signed and verified today?
- How will npm packages be signed and verified?
- Help!



How are npm packages signed today?



~~How are npm packages signed today?~~

What problem are we trying to solve?



~~How are npm packages signed today?~~

What problem are we trying to solve?

- Users are bad at managing keys



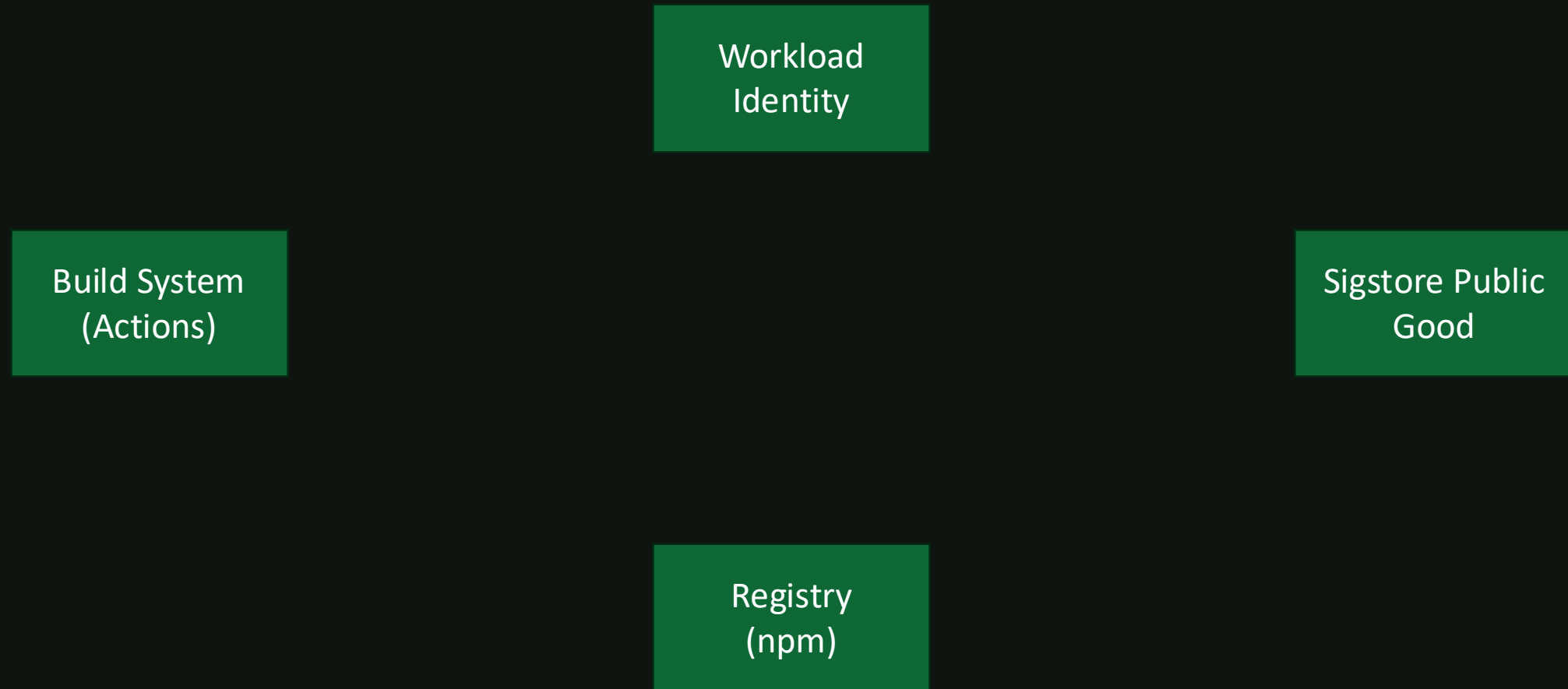
~~How are npm packages signed today?~~

What problem are we trying to solve?

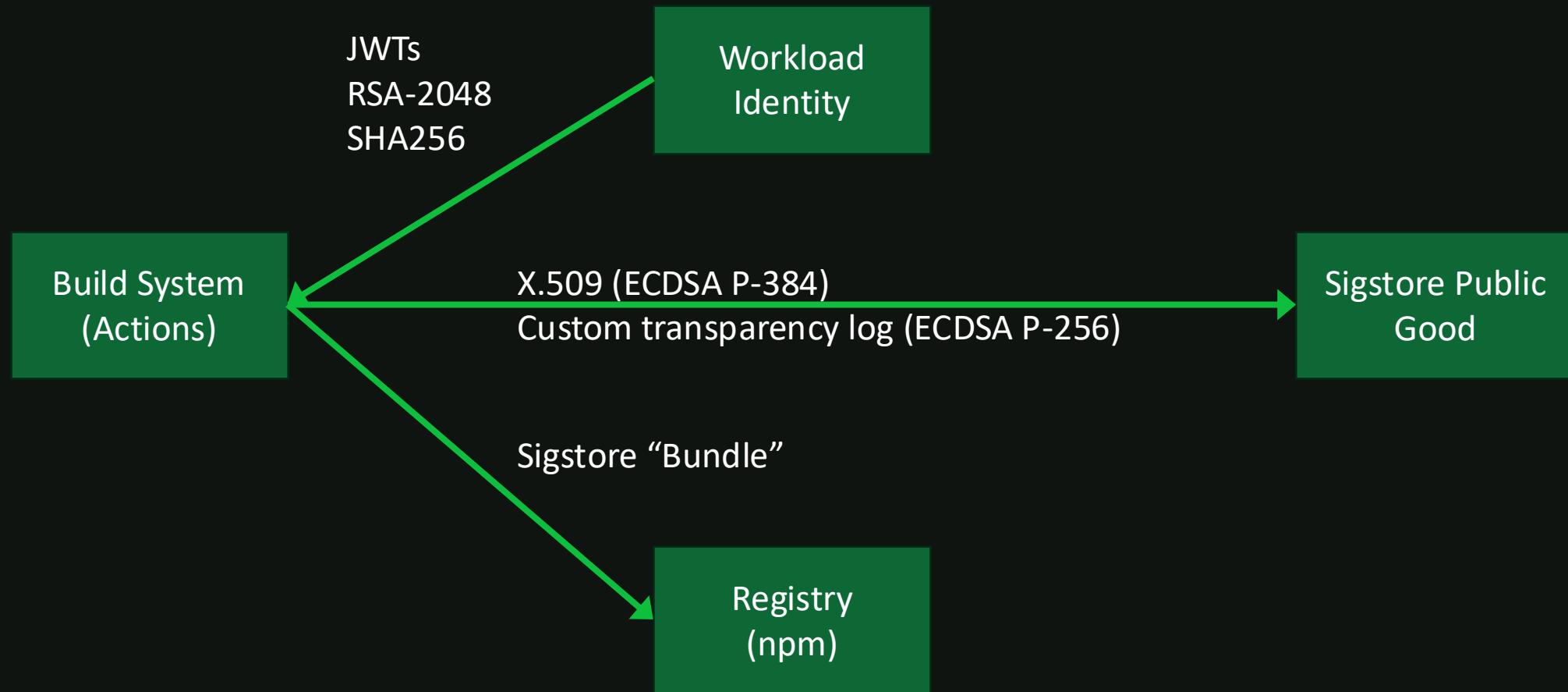
- Users are bad at managing keys
- Keys both for signing and publishing packages



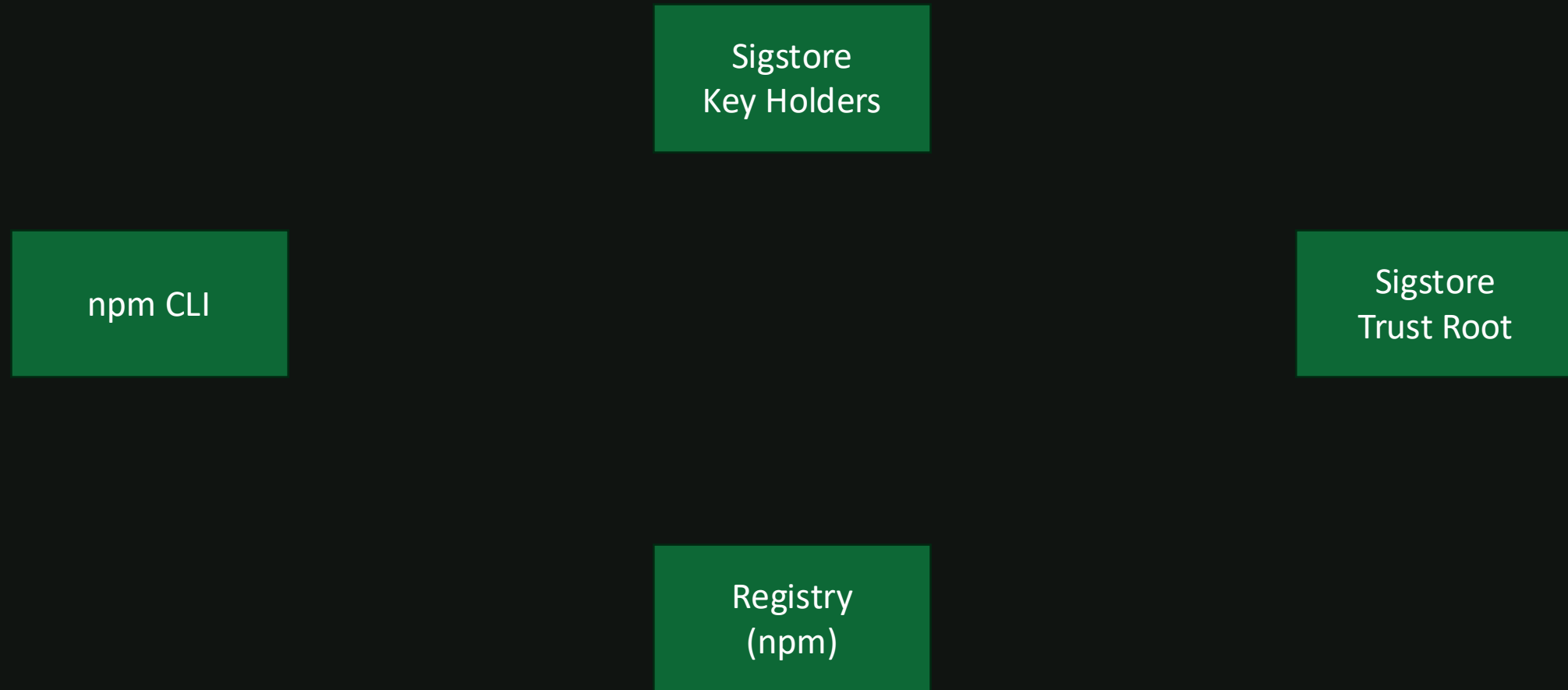
How are npm packages signed today?



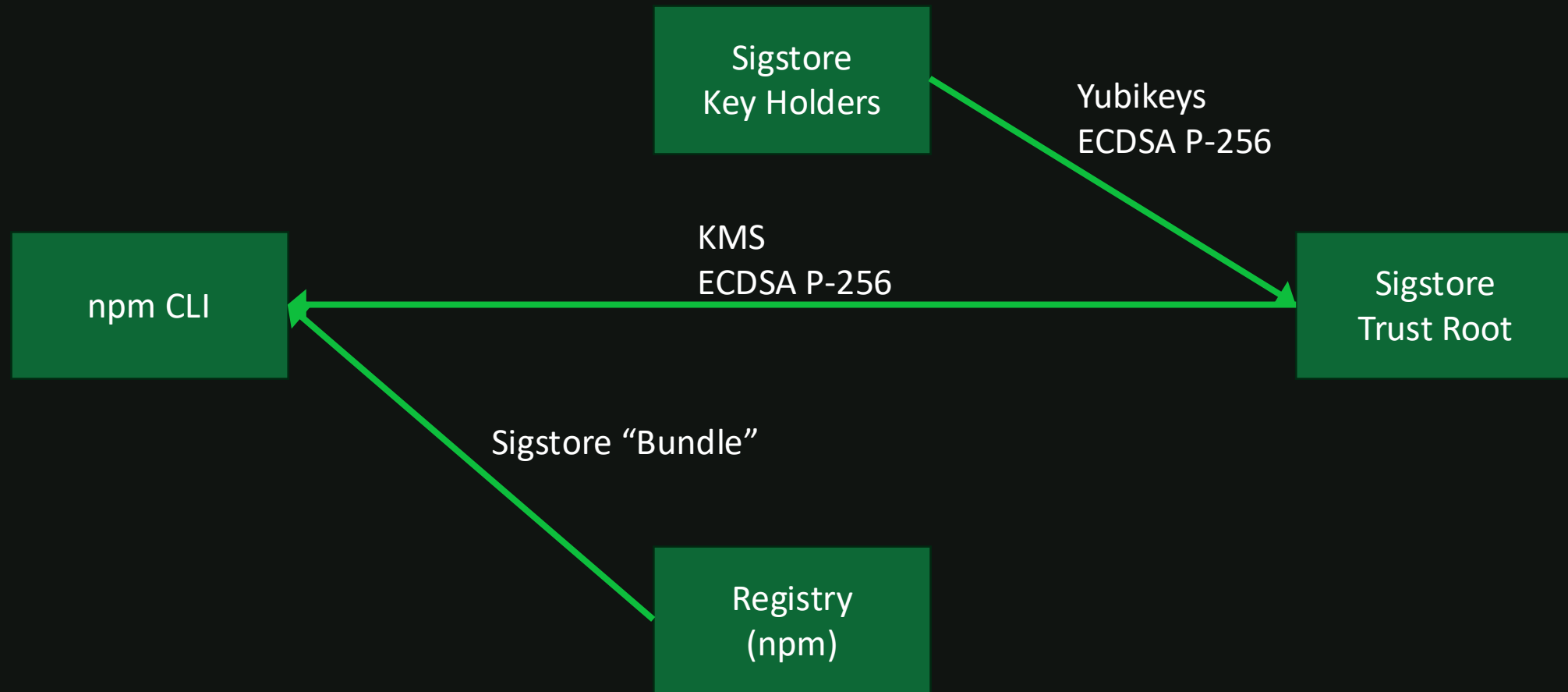
How are npm packages signed today?



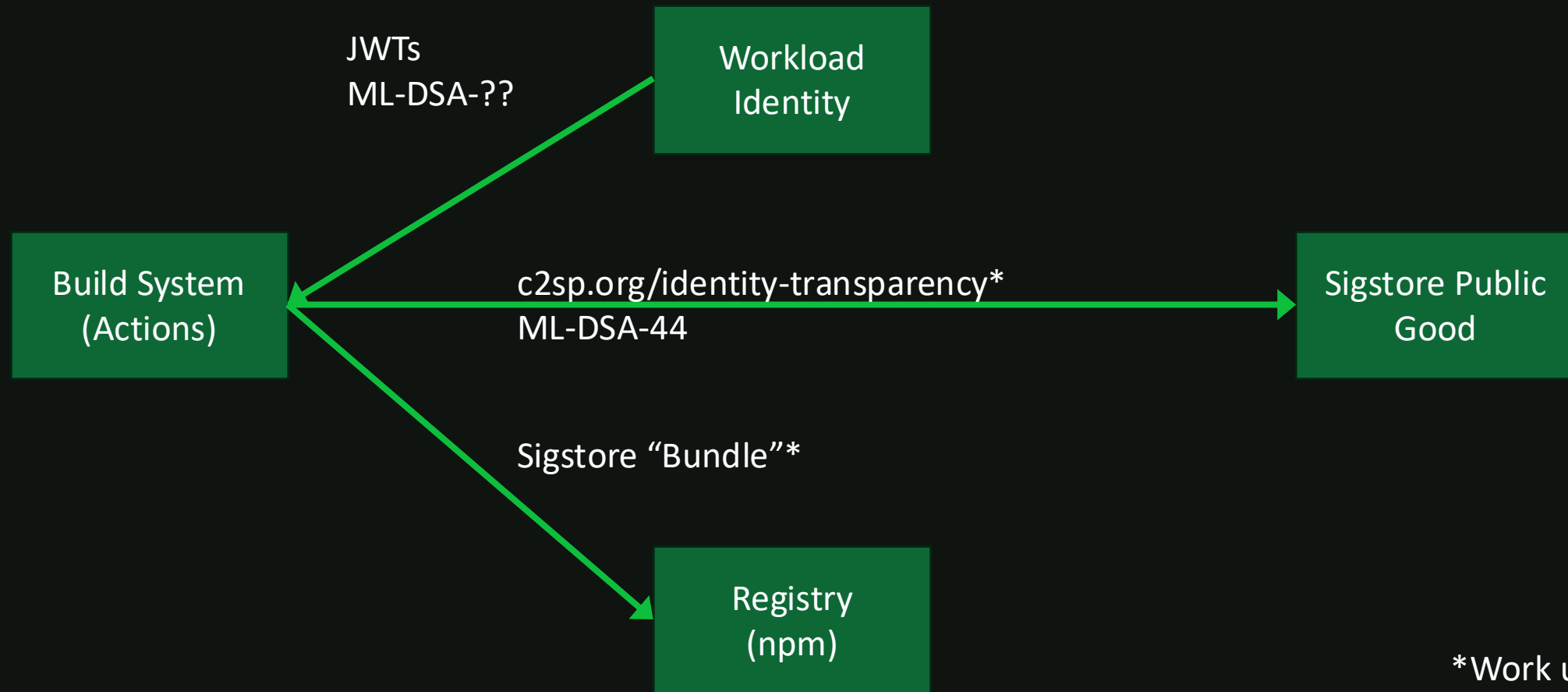
How are npm packages verified today?



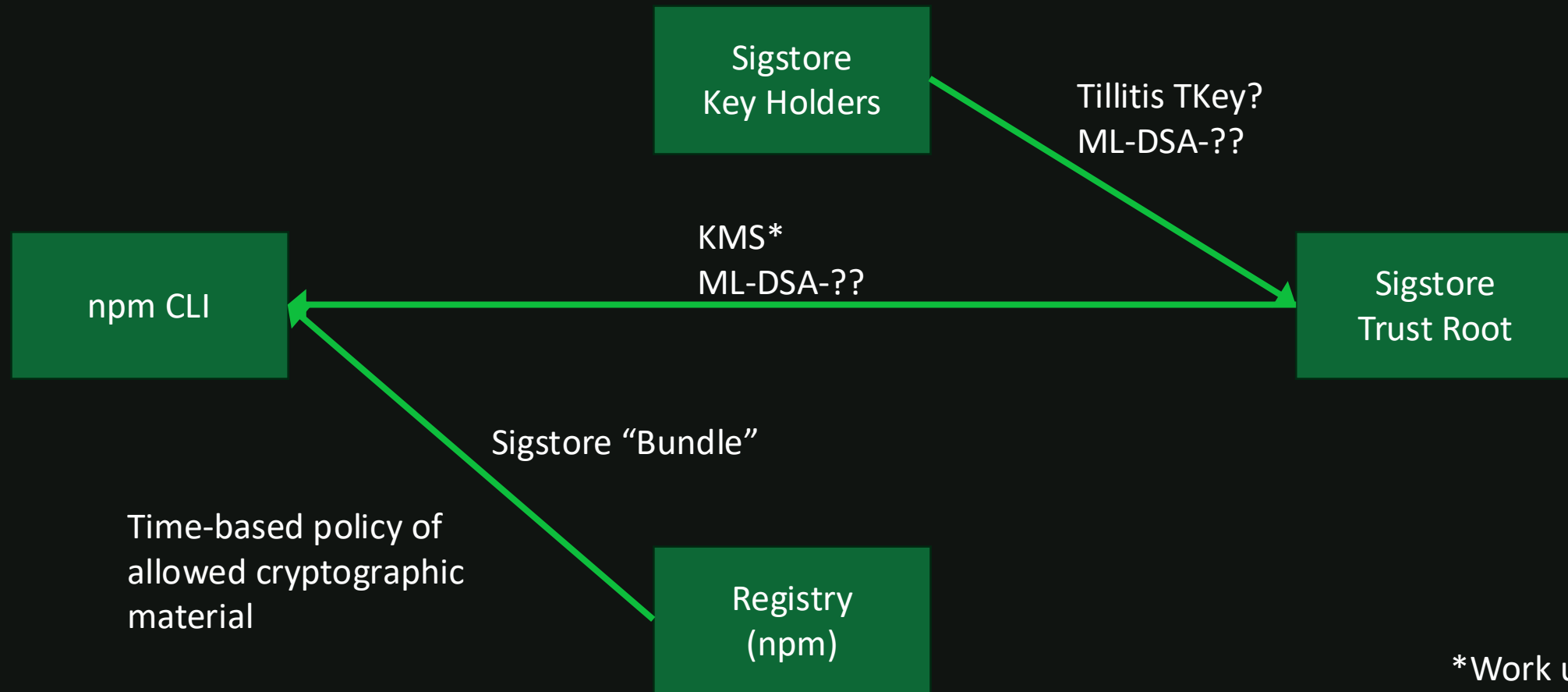
How are npm packages verified today?



How will npm packages be signed?



How will npm packages be verified?



Help!

- PQC JWTs
- PQC hardware keys
- Sigstore / TUF specifications (and then pull requests)
- What are we missing?

