



## Core Tor progress report - May 2015

[Core Tor progress report - May 2015](#)

[Guard nodes improvements: \(4.1.\)](#)

[Public key improvements: \(4.2\)](#)

[DoS resistance: \(4.3\)](#)

[Internals Documentation \(4.4\):](#)

### **Guard nodes improvements: (4.1.)**

All requirements and use-cases for guard node migrations and responses to guard filtering/DoS attacks are now enumerated, and we've begun to solidify plans for what should happen in each case. We have initial algorithm designs under consideration here; we hope to have solid algorithm writeups in June.

### **Public key improvements: (4.2)**

Reviewed, fixed bugs in, and merged #12498<sup>1</sup>, covers the core of proposal 220<sup>2</sup>. This gives every Tor server an ed25519 identity key, implements all new certificate and message types, makes servers manage their keys correctly, and makes these keys get transmitted through the directory system.

Major features (Ed25519 identity keys: #12498, Prop220):

- All relays now maintain a stronger identity key, using the Ed25519 elliptic curve signature format. This master key is designed so that it can be kept offline. Relays also generate an online signing key, and a set of other Ed25519 keys and certificates. These are all automatically regenerated and rotated as needed.
- Directory authorities track which Ed25519 identity keys have been used with which RSA1024 identity keys, and do not allow them to vary freely.
- Directory authorities now vote on Ed25519 identity keys along with RSA1024 keys.

---

<sup>1</sup> <https://trac.torproject.org/projects/tor/ticket/12498>

<sup>2</sup> <https://gitweb.torproject.org/torspec.git/tree/proposals/220-ecc-id-keys.txt>

- Microdescriptors now include ed25519 identity keys.

Major features (onion key cross-certification: #12499<sup>3</sup>):

- Relay descriptors now include signatures of the identity keys using the TAP and tor onion keys. This allows relays to prove ownership of their own onion keys. Because of this change, microdescriptors no longer need to include RSA identity keys. Implements proposal 228<sup>4</sup>;

Code simplification and refactoring:

- The link authentication code has been refactored for better testability and reliability. It now uses code generated with the "trunnel" binary encoding generator, to reduce the risk of bugs due to programmer error. Done as part of ticket 12498.

Testing:

- The link authentication protocol code now has extensive tests.
- The relay descriptor signature testing code now has extensive tests.

Updated pending patch for offline key storage and encrypted master key storage. This is under review now. It will get merged in June, we expect. (#13642<sup>5</sup>)

Implemented more code for certificate exchange and verification and authentication for ed25519 identities. Refactored authentication backend to make it easier to multithread in the future. This should also land in June, #15055<sup>6</sup>.

### **DoS resistance: (4.3)**

Released 0.2.7.1<sup>7</sup>, containing:

- Make it harder for attackers to overload hidden services with introductions, by blocking multiple introduction requests on the same circuit. Resolves ticket 15515<sup>8</sup>.
- In June, we will aim to finish a design proposal for a DoS response to Tor directory nodes, including short-term response options and longer-term response options.

### **Internals Documentation (4.4)**

No significant work in this area in May.

---

<sup>3</sup> <https://trac.torproject.org/projects/tor/ticket/12499>

<sup>4</sup> <https://gitweb.torproject.org/torspec.git/tree/proposals/228-cross-certification-onionkeys.txt>

<sup>5</sup> <https://trac.torproject.org/projects/tor/ticket/13642>

<sup>6</sup> <https://trac.torproject.org/projects/tor/ticket/15055>

<sup>7</sup> <https://blog.torproject.org/blog/tor-0271-alpha-released>

<sup>8</sup> <https://trac.torproject.org/projects/tor/ticket/15515>