Bor

Bor

Enterprise Linux Desktop Policy Management

Open-source · Self-hosted · Linux-first

TuxCon 2026 · 16–17 May, Plovdiv, Bulgaria

Policy management for Linux desktops

Who am I?



Blagovest Petrov

DevOps / Platform Engineering

- Active open source community user
- Currently working in an enterprise company

📧 blagovest@petrovs.info · 🌐 petrovs.info

What is Bor?

Core capabilities

- Policy management & distribution
- Token-based agent enrollment (or Kerberos)
- Fleet visibility — node groups & compliance
- Real-time updates via gRPC streaming
- Tamper detection in real time — managed files are watched continuously and restored instantly if modified outside Bor

The Problem

Linux management is fragmented

- Active Directory–centric tooling assumes Windows; Linux is an afterthought
- MDM & identity solutions are **expensive** or **cloud-only**
- IaC tools (Ansible, Puppet) are powerful but not built for continuous desktop enforcement

What Bor is NOT

- A **domain controller** — it does not replace FreeIPA, Samba/AD, or LDAP
- An **IaC tool** — it is not Ansible, Puppet, or Salt; those handle provisioning, Bor handles continuous enforcement
- An **orchestrator** — it is not a provisioning and lifecycle tool like Foreman

> Bor fits *alongside* your existing toolchain as the policy enforcement plane on each endpoint.

Key Features

- LINUX-FIRST designed for Linux
- SELF-HOSTED your data never leaves your infra
- OPEN SOURCE LGPLv3 — inspect, fork, contribute
- Integrates with **FreeIPA**, **Active Directory**, LDAP
- Modern stack: **Go** + **gRPC** + **PatternFly React**
- Lightweight agent — a single static binary
- Privacy & data sovereignty by default
- Native packages: deb, rpm, apk, Arch Linux
- Audit logging — all server-side events (policy changes, enrollments, user actions) and agent tamper alerts are recorded with user, IP, and timestamp

Security First

Crypto & PKI

Role	Algorithm	Lifetime
Internal CA	ECDSA P-384	10 yr
Server TLS cert	ECDSA P-256	365 d
Agent client cert	ECDSA P-256	90 d (auto-renewed)

- TLS 1.3 on agent port, mTLS mandatory
- CA auto-generated on first boot
- Optional PKCS#11 HSM for CA private key

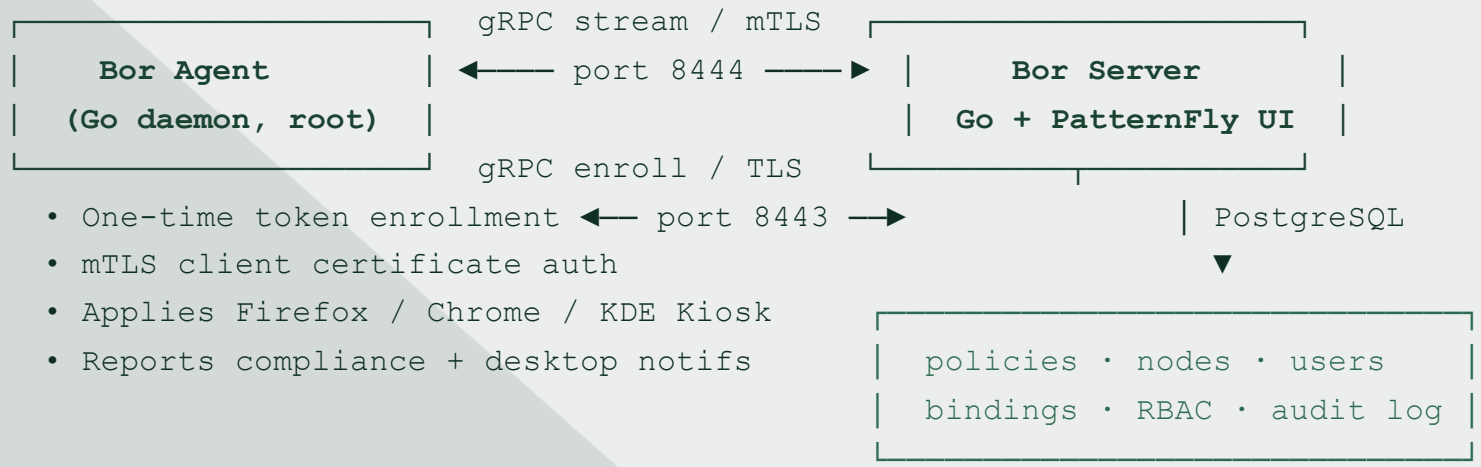
Standards

- FIPS 140-3 validated crypto
  (`GOFIPS140=v1.0.0`, CAVP A6650)
- BSI TR-02102-1 (2024)
- NIS2 / eIDAS ready

Access control

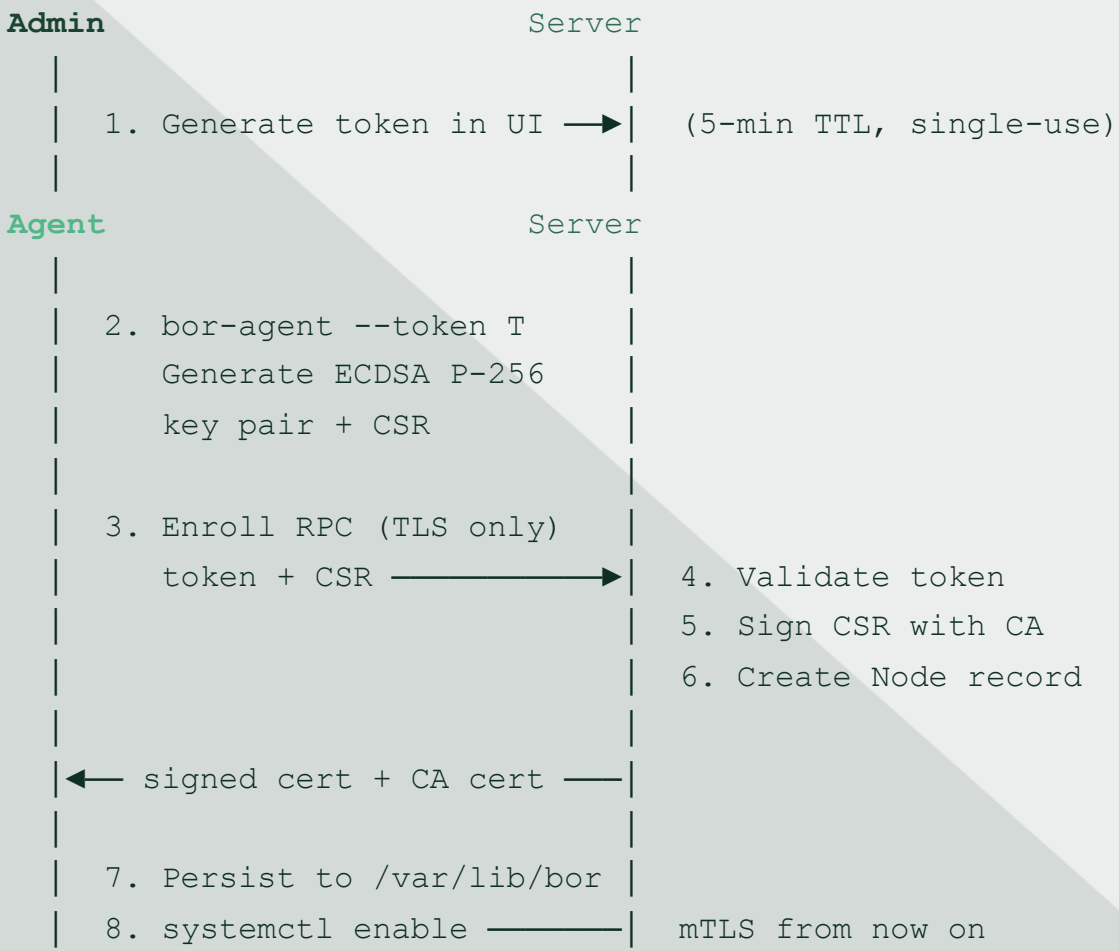
- RBAC — granular per-resource permissions
- LDAP / AD authentication
- TOTP MFA + WebAuthn / FIDO2
- Full audit log

Architecture



Default Port	Purpose	TLS	Client cert
8443	Admin UI (REST) + enrollment gRPC	TLS 1.3+	Optional
8444	Agent policy stream + cert renewal	TLS 1.3	Mandatory, mTLS

Enrollment Flow



Agent generates its own key — the private key **never leaves the machine**

Token is tied to a **Node Group** — policies start flowing immediately

Certs auto-renew every **90 days** — zero operator action needed

Kerberos enrollment: on domain-joined machines, the one-time token is replaced by a Kerberos ticket — the agent authenticates automatically using the machine's existing domain credentials, requiring no manual token generation

Supported Policy Types

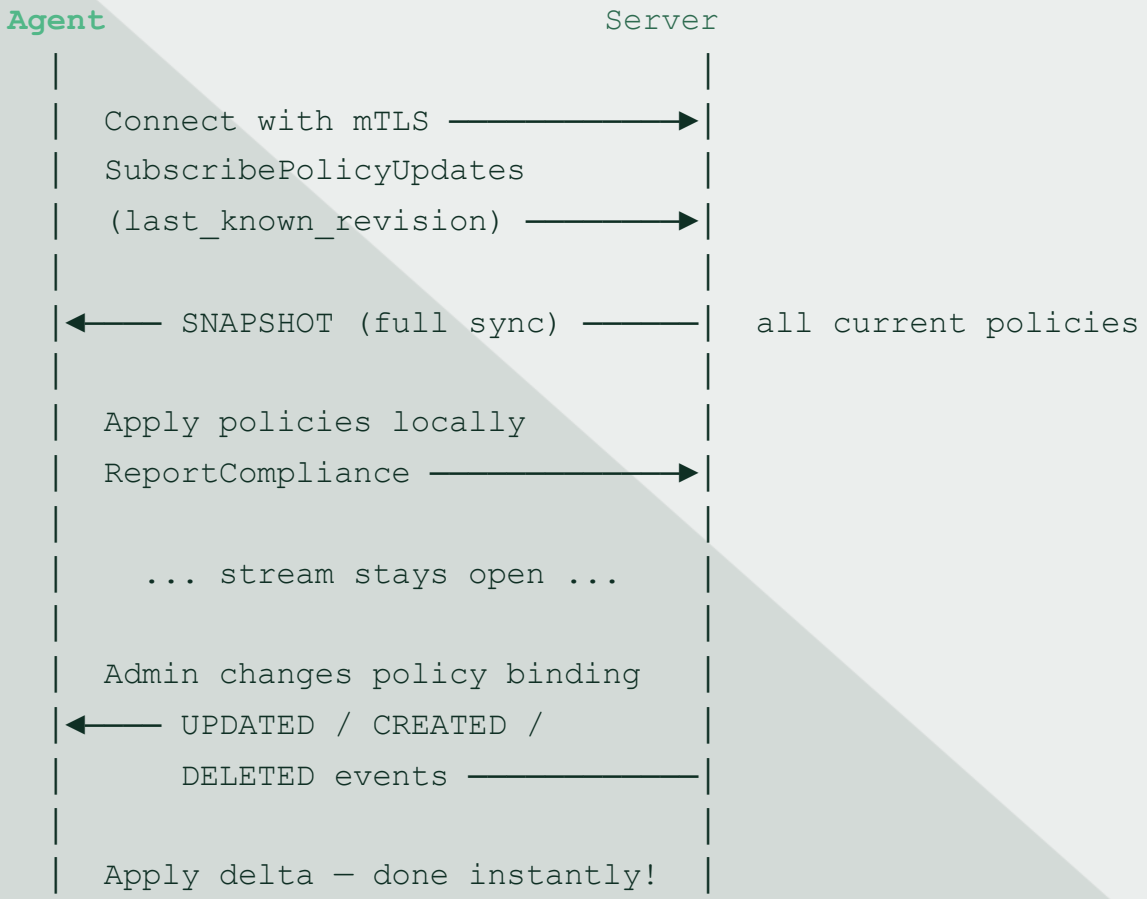
- Firefox ESR
- Chromium / Google Chrome
- KDE KConfig (Kiosk framework)
- GNOME dconf
- Polkit
- Support of Flatpak apps

Planned Policy Types

- Package management — dnf, zypper, apt, and more
- FirewallD
- Flatpak package management
- XDG Desktop Portals
- systemd services
- systemd timers

> More to come — pull requests and ideas are always welcome!

Real-Time Policy Delivery



PolicyHub

- In-memory pub/sub ring buffer
- 1 000-event window
- Monotonic revision counter

Delta sync

- Reconnecting agents get only what changed
- Full snapshot if revision too old
- Reconnect with exponential backoff (max 60 s)

Policy conflicts

- Each binding carries a **priority** value — when two policies set the same key, the higher-priority one wins

Roadmap *(Help is appreciated!)*

- Agent auto-update mechanism
- Multi-tenancy
- Policy import/export format
- Sync policies with Git
- ACME protocol support (Let's Encrypt)
- Documentation, documentation, documentation…
- E2E testing + use cases
- I18n

Get Involved

🌐 getbor.dev

🐙 github.com/VuteTech/Bor

✉️ blagovest@petrovs.info

🗂️ getbor.dev/publications/tuxcon2026

Contribute

Issues, PRs, feedback — all welcome. See `docs/CONTRIBUTING.md`

Spread the word

Star ⭐ the repo and share with your Linux admin friends.

Licensed under LGPLv3 · Copyright © 2026 Vute Tech LTD & contributors



Time for a Demo