Gimel Foundation

Gimel Foundation gGmbH i.G.
GiFo-Request for Comments: 0400
Obsoletes: -
Category: Standards Track

Dr. Goetz G. Wehberg
Digital Supply Institute
15. Februar 2026

Robot Authorization Protocol 1.0 (G-ROS)

Abstract

The Robot Authorization Protocol (G-ROS) enables comprehensive authorization enforcement for autonomous robots by bridging IT-level authorization with physical hardware enforcement. G-ROS introduces Context Based Power-of-Attorney Control (CBPC) for real-time, context-dependent authority management of physical and non-physical robot actions.

G-ROS extends the GAuth authorization framework (GiFo-RFC-0110, GiFo-RFC-0111) from the digital domain into physical robotics, introducing hardware-level Embedded Enforcement Points (EEPs) that enforce authorization constraints at the actuator level using Control Barrier Functions (CBFs). The protocol can operate in two complementary modes: Rule-Based Enforcement via GAuth with Power of Attorney (PoA) Maps for explicit authority [Subject to GiFo-RFC-0400], and AI-Based Enforcement via G-Agent for evaluating implied authority [Excluded from GiFo-RFC-0400 in line with Exclusions].

G-ROS builds on the Robot Operating System 2 (ROS 2) ecosystem and its DDS-Security infrastructure, adding behavioural authorization, continuous compliance monitoring, and embedded safety enforcement.

Status of This Memo

This is a Gimel Foundation Standards Track document.

This document is a product of the Gimel Foundation (GiFo). It represents the current consensus of the Gimel Foundation community. It has performed review and has been approved for publication.

Information about the status of this document, any errata, and how to provide feedback on it may be obtained at https://gimelfoundation.com or https://github.com/Gimel-Foundation.

Legal notice

This document is subject to the Gimel Foundation's Legal Provisions Relating to GiFo Documents (see http://GimelFoundation.com or https://github.com/Gimel-Foundation) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include License text as described in Section 4. of the GiFo Legal Provisions Relating to Gimel Foundation Documents and are provided without warranty as described in the Provisions and its respective license conditions.

The distinguished G-ROS standard is protected by copyright and patent law (patent pending). G-ROS is an open-source standard building on GAuth and extending it to physical robotics. G-ROS must not use Exclusions (see Scope), which are subject to separate license conditions and are also protected by copyright as well as patent law (patent pending).

Implementations of G-ROS must refer to the following licenses and specifications in line with their respective license conditions:

- The Apache 2.0 license of ROS 2, provided by Open Robotics / Open-Source Robotics Foundation
- The OMG specification license of DDS (Data Distribution Service, v1.4) and DDS-Security (v1.2)
- The Apache 2.0 license of GAuth (GiFo-RFC-0110, GiFo-RFC-0111) and PoA-Definition (GiFo-RFC-0115), provided by Gimel Foundation (incl. Exclusions)
- The Apache 2.0 license of GAuthent (GiFo-RFC-0300), provided by Gimel Foundation (incl. Exclusions)
- The Apache 2.0 license of OAuth (IETF RFC 6749, RFC 7636) and OpenID Connect, in line with their respective license conditions
- The MIT license of MCP (Model Context Protocol), in line with its license conditions

Copyrights and licenses of these building blocks apply accordingly.

Implementations of G-ROS must be licensed with Apache 2.0, granted by Gimel Foundation, and must not integrate Exclusions (as per Scope statement of this Request for Comment). Defined Exclusions of G-ROS must refer to separate license conditions.

Notational Conventions

The key words "Must", "Must Not", "Required", "Shall", "Shall Not", "Should", "Should Not", "Recommended", "May", and "Optional" in the following specification are to be interpreted as described in the Internet Engineering Taskforce`s (IETF) RFC 2119.

Credits

We would like to express our sincere gratitude to Dr. Jan-Christian Schütte for his invaluable contributions to the patent filing and intellectual property development underlying the G-ROS protocol. His expertise in patent law and technology protection has been essential to securing the foundational innovations described in this specification.

Table of Contents

***

1. Scope

G-ROS concerns the technical field of robotics authorization and AI governance applied to physical autonomous systems. With the increasing deployment of autonomous robots in manufacturing, logistics, healthcare, transportation, and domestic environments, there is a critical need for comprehensive authorization protocols that govern not only what robots may access but also what physical (or non-physical) actions they may perform, under what conditions, and with what force, speed, and spatial boundaries.

G-ROS extends the GAuth authorization framework from the IT/digital domain into physical robotics by introducing hardware-level enforcement of authorization constraints. While GAuth (GiFo-RFC-0110, GiFo-RFC-0111) addresses the question of AI authorization for digital agents, G-ROS answers the additional questions specific to physical robots: Where may this robot operate? How fast may it move? What forces may it apply? Under what environmental conditions? And critically, how are these physical constraints enforced at the hardware level to prevent software compromise from bypassing safety limits?

G-ROS builds on the following standards as building blocks:

- GAuth 0.1 (GiFo-RFC-0110), provided under Apache 2.0 by Gimel Foundation
- GAuth 1.0 (GiFo-RFC-0111), provided under Apache 2.0 by Gimel Foundation
- PoA-Definition (GiFo-RFC-0115), provided under Apache 2.0 by Gimel Foundation
- GAuthent 1.0 (GiFo-RFC-0300), provided under Apache 2.0 by Gimel Foundation
- ROS 2, provided under Apache 2.0 by Open Robotics / OSRF
- DDS v1.4 and DDS-Security v1.2, OMG specifications
- Control Barrier Function (CBF) theory from academic literature
- OAuth (IETF RFC 6749, RFC 7636) and OpenID Connect
- MCP (Model Context Protocol), provided under MIT license

2. Limitations on the right to make derivative works (Exclusions)

G-ROS is freely available as an open-source solution based on Apache 2.0 with the following Exclusions. Users of G-ROS Must Not - whether directly or indirectly - integrate G-ROS with:

- DNA-based identities or identities based on genetic data, respectively, which offer particularly secure biometrics (e.g., Gimel ID),
  - incl. AI that tracks the quality of DNA-based identities
  - incl. AI that tracks risks in terms of identity theft or any other risks.

- The use of AI or AI operators for running, controlling, or orchestrating the G-ROS protocol, i.e.,
    - AI that controls the entire process (or parts of it) of a robot authorization deployment life cycle
    - AI that tracks actions and/or decisions regarding authorization compliance (e.g., implied authority tracking, G-Agent intelligence)
    - AI that assures the quality of the outcome of robot authorization engagements.
- The use of Web3, i.e., blockchain technology (including respective web3 tokens and smart contracts) for authorization tokens, PoA Map storage, or enforcement coordination or anything attached to it.

These Exclusions are excluded from the G-ROS open-source standard. Users Must Not use, integrate or add all or some of these Exclusions in any form to the G-ROS standard without a separate licensed permission in writing. Users Must exclude these Exclusions from any implementation of G-ROS unless licensed separately. Gimel Technologies GmbH offers separate solutions for this purpose, e.g. in terms of Gimel ID, G-Agent and Gimel ROS. These separate solutions are being protected by copyright and patent law (patent pending).

In this context it is worth mentioning that any robot or agentic AI to be authorized can comprise a lead AI and at least one team AI. The G-ROS standard Must only be applied for centralized authorization, i.e., all robots and AI units Must be authorized centrally by G-ROS. The transfer of authorization authority to the AI lead or any other component of the robotics system Must Not be deployed and is subject to the Exclusions of the G-ROS standard. Any AI-controlled G-ROS protocol Must be licensed additionally under separate license conditions in line with the Exclusions of this specification.

In line with GiFo-RFC0090, Gimel Foundation May revoke at its sole discretion the rights and licenses granted to a user with respect to Contributions and Documents, if the user does not use Contributions and Documents in line with Legal Provisions of Gimel Foundation.

3. Glossary of key terms and expressions associated with G-ROS

Essential nomenclature used in this document is defined as follows. The definitions Should Not be understood as limiting the scope of application or technical variants, but rather as pointers to some ways of understanding implementations of G-ROS.

G-ROS (Gimel Robot Operating System): An independent robot governance and control system that bridges IT authorization (GAuth) with physical hardware enforcement for autonomous robots.

CBPC (Context Based Power-of-Attorney Control): A permission model where authorization grants are functions of real-time context rather than static scopes.

G-Agent: The AI-based component responsible for evaluating implied authority. [Excluded from GiFo-RFC-0400 in line with Exclusions]

EEP (Embedded Enforcement Point): A dedicated hardware component positioned between the robot's compute unit and its actuators. Cannot be bypassed by software.

PoA Map (Power of Attorney Map): A structured, machine-readable representation of a robot's delegated authority, extending GiFo-RFC-0115.

GAuth (Gimel Authorization Protocol): The authorization protocol specified in GiFo-RFC-0110 and GiFo-RFC-0111 that G-ROS extends to physical robotics.

Control Barrier Functions (CBFs): Mathematical functions that define safety invariants. In G-ROS, CBFs are implemented in EEP hardware.

P*P Architecture (Power*Point): The abstract role architecture within GAuth: PEP, PDP, PIP, PAP, and PVP.

Explicit Authority: Authorization defined through explicit rules and clear metrics in PoA Maps. Enforced deterministically through EEPs and CBF filters.

Implied Authority: Authorization inferred through AI-based evaluation of whether robot behaviour aligns with the spirit of granted permissions. [Excluded from GiFo-RFC-0400 in line with Exclusions]

HSM (Hardware Security Module): A dedicated cryptographic processor for secure key storage, identity attestation, and boot chain verification.

Authority Disclosure: A characteristic enabling a robot to disclose its power of attorney to any relying party upon request.

Extended Token: As defined in GAuth — in G-ROS, additionally carries embedded CBF constraint parameters for hardware enforcement.

4. G-ROS architecture overview

G-ROS operates in two complementary authorization modes. The Rule-Based mode is the core open-source specification. The AI-Based mode (G-Agent) is referenced for architectural completeness but is subject to Exclusions.

4.1 Dual-Mode Enforcement

Mode	Authorization Type	Status in RFC-0400
Rule-Based (G-ROS Core)	Explicit Authority via PoA Maps, EEPs, CBF filters	Open-source specification (this document)
AI-Based (G-Agent)	Implied Authority via learned behavioral patterns	*[Excluded from GiFo-RFC-0400 in line with Exclusions]*

Rule-Based Authorization (Explicit Authority): The core G-ROS framework operates on explicit authority grants defined through PoA Maps. Constraints such as "maximum velocity 2.0 m/s" or "permitted zones: warehouse_floor" are enforced deterministically through EEPs at the hardware level and CBF filters at the control level. This mode provides mathematically provable safety guarantees.

AI-Based Authorization (Implied Authority): The G-Agent component handles situations where explicit rules cannot anticipate all valid operational scenarios. [Excluded from GiFo-RFC-0400 in line with Exclusions] The architectural position of G-Agent is described for completeness, but all AI-based implied authority evaluation is excluded from the open-source specification.

4.2 Architecture Layers

Layer	Mode	Component	Latency	RFC-0400 Status
L0: Hardware	Rule-Based	EEP	< 100 μs	Specified
L1: Control	Rule-Based	CBF Safety Filter	< 1 ms	Specified
L2: Execution	Rule-Based	G-ROS Node Wrappers	< 10 ms	Specified
L3: Planning	Rule-Based	Authorized Planner	< 100 ms	Specified
L4: Mission	Rule-Based	Mission Controller	< 1 s	Specified
L5: Cloud	AI-Based	G-Agent (Cloud)	< 10 s	*[Excluded from GiFo-RFC-0400 in line with Exclusions]*
L5a: Edge	AI-Based	Edge G-Agent	< 500 ms - 2 s	*[Excluded from GiFo-RFC-0400 in line with Exclusions]*
L6: Governance	Both	GAuth Server	Min-hours	Specified

4.3 Three-Layer Integration

- GAuth Cloud Authorization (L4, L6): Identity attestation, authority chains, PoA Map issuance, and audit.
- Edge Compute Layer (L2-L4): Mission lifecycle, authorization distribution to ROS 2 nodes, rule-based compliance monitoring.
- Hardware Enforcement Layer (L0-L1): EEP and CBF Safety Filter enforce physical constraints with sub-millisecond latency.

Note: AI-based implied authority assessment at L5/L5a (G-Agent) is [Excluded from GiFo-RFC-0400 in line with Exclusions].

4.4 Integration with ROS 2

ROS 2 Component	Specification	G-ROS Extension
DDS Middleware	OMG DDS 1.4, RTPS 2.3	GAuth token transport via DDS user data
Security	DDS-Security 1.2, SROS2	Extended permissions with PoA Map enforcement
Node Lifecycle	REP-2007	GAuth validation at state transitions
Actions	REP-2008	Continuous authorization during execution
Parameters	ROS 2 Parameter API	CBF parameters from GAuth tokens
Logging	rcl_logging	Cryptographically attested audit logs
QoS	DDS QoS Policies	Authorization-aware QoS enforcement

5. Context Based Power-of-Attorney Control (CBPC)

CBPC is the core permission model of G-ROS. Unlike traditional access control models that grant static permissions, CBPC represents permissions as functions of real-time context. A CBPC might specify: "navigate within zone A at speeds up to 2 m/s when pedestrian density is below threshold T, reducing to 0.5 m/s otherwise." The robot's embedded enforcement layer evaluates these contextual conditions continuously without requiring cloud roundtrips.

5.1 PoA Maps for Robots

PoA Maps extend the PoA-Definition of GiFo-RFC-0115 for physical robots, consisting of three main sections:

Section	Category	Attributes
A. Parties	Principal / Authorizer / Client	Identity, organizational role, robot identity and capabilities
B. Type & Scope	Authorization scope	Representation type, applicable sectors (ISIC/NACE), regions, authorized actions
C. Requirements	Operational constraints	Validity, limits of powers, rights & obligations, security, jurisdiction

5.2 PoA Map Operational Layers

Layer	Description	Example Constraints
L1: Spatial	Geographic boundaries	Geofences, exclusion zones, altitude limits
L2: Temporal	Time restrictions	Operating hours, maintenance windows
L3: Kinematic	Motion constraints	Velocity limits, acceleration bounds
L4: Dynamic	Force constraints	Contact force limits, payload restrictions
L5: Interaction	Human interaction	Approach distances, handoff protocols
L6: Task	Permitted operations	Allowed manipulations, navigation goals
L7: Environmental	Condition rules	Weather limits, crowd density
L8: Mission	Objective constraints	Priority levels, abort conditions
L9: Network	Communication rules	Allowed endpoints, encryption
L10: Audit	Logging requirements	Telemetry frequency, retention

5.3 Authority Chain Narrowing

Each link in the authority chain can only narrow permissions, never expand them. No robot can ever exceed the authority of its most restrictive authorizer.

5.4 GAuth Token Structure for Robots

The GAuth extended token embeds the PoA Map alongside technical enforcement parameters. GAuth for G-ROS is specified in GiFo-RFC0401 (standalone) and GiFo-RFC0402 (OAuth-compounding).

6. Embedded Enforcement Point (EEP)

The EEP is a dedicated hardware component positioned physically between the robot's main compute unit and its actuators. Every control signal must pass through the EEP before reaching physical hardware. The EEP operates on its own secure boot chain and can only be updated via cryptographically signed firmware.

6.1 EEP Specifications

Characteristic	Specification
Processing Speed	1000+ Hz control loop, < 100 µs latency
Constraint Types	Velocity, force/torque, spatial boundaries, acceleration caps
Enforcement Method	Control Barrier Functions (CBFs) with mathematical safety invariants
Update Mechanism	Cryptographically signed firmware only
Failure Mode	Fail-safe: defaults to most restrictive constraints
Hardware Examples	STM32H7 + FPGA, Xilinx Zynq, NXP i.MX RT

6.2 Enforcement Pipeline

When a motor command arrives at the EEP: (1) verify the command originates from an authenticated source, (2) evaluate against loaded CBF constraints, (3) if compliant, pass to actuator unchanged, (4) if non-compliant, clamp to nearest safe value or block entirely, (5) log the violation and report to the Mission Controller.

6.3 Bypass Resistance

The EEP cannot be bypassed, reprogrammed, or disabled by software. A robot moving at 2 m/s covers 2 mm per millisecond — network latency of 50 ms translates to 10 cm of potentially uncontrolled motion. This architecture satisfies ISO 13849 and IEC 62443 requirements.

6.4 Latency Tiers

Tier	Latency	Component	Function
L0: CBF Core	< 100 μs	EEP FPGA/MCU	Motor command clamping
L1: Joint Limits	< 1 ms	CBF Safety Filter	Position, velocity, torque limits
L2: Collision Avoidance	< 10 ms	G-ROS Node Wrappers	Proximity-based speed reduction
L3: Zone Enforcement	< 100 ms	Authorized Planner	Geofence compliance
L4: Path Validation	< 1 s	Mission Controller	Trajectory authorization

7. G-Agent and Confidence-Based Escalation

This entire section describes capabilities that are excluded from GiFo-RFC-0400 in line with Exclusions. It is shared to provide a more extended architectural view of the G-ROS system. Implementations of G-ROS Must Not include G-Agent or any AI-based implied authority evaluation without separate license.

G-Agent is the AI-based component responsible for evaluating implied authority: determining whether robot actions not explicitly authorized nonetheless align with the operator's intent. G-Agent operates in a tiered architecture:

Tier	Location	Latency	Scope
Edge Cache	Robot / Local	< 500 ms	Pre-computed authority playbooks
Edge Inference	Facility Gateway	< 2 s	Distilled AI model (<500MB)
Cloud G-Agent	Cloud	< 10 s	Full JEPA model with complete context

G-Agent employs confidence-based escalation to route decisions to the appropriate tier. A fundamental principle: G-Agent cannot override the hard safety constraints enforced by the EEP at layers L0-L1.

All capabilities described in this section — including JEPA-based learning, confidence-based escalation, authority playbooks, edge inference, and behavioural pattern recognition — are excluded from GiFo-RFC-0400 in line with Exclusions.

8. Security and Threat Model

8.1 Threats Mitigated

Threat	Attack Vector	G-ROS Defense
LLM Jailbreaking	Manipulating AI to bypass safety	EEP enforces constraints independently of AI
Spoofed PoA Commands	Forged authorization tokens	Cryptographic chain verification via HSM
Replay Attacks	Reusing captured tokens	Temporal validation, nonce-based tokens
PoA Map Forgery	Fake authority grants	Authority chain attestation
Privilege Escalation	Expanding permissions	Authority chains only narrow, never expand
Firmware Tampering	Modifying EEP logic	Secure boot, signed firmware only

8.2 Defence Against LLM-Based Attacks

Prompt Injection: EEP validates all commands against PoA Map independently of the AI layer.

Hallucination-Induced Actions: GAuth request-approval cycle independently evaluates requests against PoA constraints.

Data Poisoning: EEP's CBFs define mathematically proven safety invariants that cannot be overridden by software.

Indirect Prompt Injection: Environmental inputs cannot expand permissions. The PoA Map is established through cryptographic human-verified delegations.

Multi-Turn Manipulation: Authority chains can only narrow, never expand. Each request evaluated against original PoA grant.

Note: Advanced AI-based threat detection (G-Agent monitoring for goal drift, fleet-wide attack pattern detection) is excluded from GiFo-RFC-0400 in line with Exclusions.

9. Hardware Reference Architectures

Robot Class	HSM	EEP	Compute	Constraints
Humanoid	Infineon OPTIGA	Multi-limb EEPs	NVIDIA Jetson, 50-200W	32+ DOF, force/torque per joint
Industrial Arm	Microchip ATECC608	Xilinx Zynq	Industrial PC, 20-50W	6-7 DOF, high force, precise workspace
Autonomous Vehicle	TPM 2.0	Redundant dual-EEP	Rack-mount, 100-500W	Velocity, steering, braking, ODD
Delivery Drone	NXP SE050	Lightweight FPGA	Qualcomm RB5, 10-20W	Altitude, geofence, wind, payload
Household Robot	Integrated HSM	NXP i.MX RT	ARM-based, 10-30W	Low force, furniture avoidance

Each architecture ensures the EEP is physically separate from the main compute unit. The HSM provides hardware-rooted identity for GAuth attestation.

10. Benefits

Practical: By combining GAuth's power-of-attorney framework with hardware-enforced safety limits, G-ROS enables relying parties to verify and trust a robot's authorized actions.

Comprehensive: G-ROS integrates IT authorization, physical enforcement, and rule-based compliance monitoring.

Verifiable: Authority Disclosure enables any relying party to verify a robot's authorization scope and the chain of human authority behind it.

Automated: Rule-based compliance monitoring enables continuous, automated enforcement of PoA Map constraints. *AI-based automated compliance assessment via G-Agent is excluded from GiFo-RFC-0400 in line with Exclusions*.

Compounding: G-ROS builds on ROS 2, DDS, GAuth, OAuth, OpenID Connect, and MCP — compounding existing infrastructure.

Upgradable: The Exclusions represent capabilities that can upgrade G-ROS: Web3, DNA-based identities, and AI-driven protocol orchestration, available under separate license from Gimel Technologies GmbH.

11. Next Steps

Detailed specifications for the following G-ROS components are being defined by subsequent specifications:

- GiFo-RFC0401: GAuth Standalone Authorization Framework for Robots
- GiFo-RFC0402: GAuth OAuth-Compounding Authorization Framework for Robots
- Detailed PoA Map attribute definitions for specific robot classes and industries
- EEP hardware certification requirements and reference implementations
- Cross-robot collaboration authorization and PoA Map intersection algorithms

New developments such as post-quantum cryptography (e.g., by NIST) and next-level AI models (e.g., JEPA from Yann LeCun) are compatible with G-ROS, yet to be considered with its implementations.

While several embodiments have been described in this document, it is understood that various modifications May be made for implementing it without departing from the spirit and scope of G-ROS.

Disclaimer: ALL DOCUMENTS AND THE INFORMATION CONTAINED THEREIN ARE PROVIDED ON AN "AS IS" BASIS AND THE CONTRIBUTOR, THE ORGANIZATION THEY REPRESENT OR ARE SPONSORED BY (IF ANY), THE GIMEL FOUNDATION, AND ANY APPLICABLE MANAGERS OF ALTERNATE DOCUMENT STREAMS, DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION THEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

* * *