DEMP Specification

DEMP-SPEC 0.6.0

9 February 2026

Table of Contents

1 Introduction

The **Decentralized Emergency Management Protocol (DEMP)** provides secure, interoperable, decentralized communication between Safety Information Systems (SIS), operating either as standalone nodes or within a Federation. It supports scalable Alert propagation and information exchange across Safety Zones, Entities and Devices, enabling real-time collaborative emergency management.

The **Decentralized Emergency Management Protocol Specification (DEMP-SPEC)** defines the architecture and implementation guidelines for emergency management built on DEMP.

1.1 Revision History

The full revision history for this specification is maintained at: `https://demp.ch/spec/CHANGELOG.md`

1.2 Source Repository

The DEMP Specification (DEMP-SPEC) is maintained on GitLab and mirrored to GitHub to support feedback, collaboration and community engagement. These public repositories provide transparency and spaces for discussing issues and tracking changes.

- Canonical Repository: `https://gitlab.com/jpgrossglauser/demp-spec`
- Mirror (read-only): `https://github.com/jpgrossglauser/demp-spec`

1.3 Versioning

This specification follows Semantic Versioning (SemVer) 2.0.0 to manage its releases and updates. Version numbers reflect changes to the specification and are intended to help stakeholders assess the impact of updates on existing implementations.

For tooling and automation purposes, the current version of this specification may also be exposed via a `VERSION` file available at `https://demp.ch/spec/VERSION`

1.4 Conformance

1.4.1 Requirement Levels

The key words **“MUST”**, **“MUST NOT”**, **“REQUIRED”**, **“SHALL”**, **“SHALL NOT”**, **“SHOULD”**, **“SHOULD NOT”**, **“RECOMMENDED”**, **“MAY”**, and **“OPTIONAL”** in this document are to be interpreted as described in RFC 2119 and RFC 8174, when, and only when, they appear in all capitals, as shown here.

2 License

3 Audience

The primary goal of this specification is to provide comprehensive documentation for **software architects, developers and integrators**, enabling them to design, implement and integrate DEMP-based systems and applications.

4 Architecture

4.1 Network

A **DEMP Network MUST** form the backbone for communication between multiple Safety Information Systems (SIS).

4.1.1 Decentralization

There **MUST** be no central authority managing the DEMP Network operations.

4.1.2 Interoperability

A DEMP Network **MUST** support interoperability between heterogeneous implementations of Safety Information Systems (SIS), ensuring that they can securely communicate with each other, regardless of their underlying hardware, software or geographical location.

4.1.3 Communication

A DEMP Network **SHOULD** rely on the Internet Protocol (IP) for communication (RFC 791, RFC 8200) and **MAY** use the Domain Name System (DNS) for naming and addressing purposes (RFC 1034, RFC 1035).

4.1.4 Scalability

A **DEMP Network MUST** be designed to scale dynamically, allowing Safety Information Systems (SIS) to be added to or removed from the network without disrupting ongoing operations or compromising availability.

4.1.5 Scope

4.1.5.1 Wide Area Network (WAN) A **DEMP Network SHOULD** be able to operate across Wide Area Networks (WAN), including the public Internet, to enable communication and federation between geographically distributed Safety Information Systems (SIS).

4.1.5.2 Local Area Network (LAN) A **DEMP Network SHOULD** be able to operate within a Local Area Network (LAN), enabling Safety Information Systems (SIS) to function autonomously in isolated, offline or network-restricted environments.

4.1.5.3 Virtual Private Network (VPN) A **DEMP Network SHOULD** support operation over Virtual Private Networks (VPN), enabling secure and controlled interconnection between geographically or administratively separate Safety Information Systems (SIS).

4.1.5.4 Ad Hoc Network A **DEMP Network MAY** support operation within a local mesh or peer-to-peer (P2P) ad hoc network that enables offline or short-range secure data exchange.

4.1.6 Discovery

4.1.6.1 Directory A DEMP Network **MAY** provide a directory to facilitate the discovery of Safety Information Systems (SIS). If provided, the directory **MUST** maintain an accurate and up-to-date registry of all participating SIS.

4.1.6.2 Participation Participation in any discovery mechanism **MUST** be voluntary. A Safety Information System (SIS) **MUST** be able to opt in to or opt out of a Network Directory without affecting its ability to operate within the DEMP Network.

4.2 Safety Information System (SIS)

A **Safety Information System (SIS) MUST** monitor, manage, process and exchange safety-related data for Entities and between Safety Information Systems (SIS), either as a standalone instance or as a participant in a Federation.

4.2.1 Data Exchange

A **Safety Information System (SIS) SHOULD** ensure reliable information exchange with Entities and other Safety Information Systems (SIS), taking availability constraints into consideration.

4.2.2 Data Processing

A Safety Information System (SIS) **MUST** process DEMP data in accordance with applicable privacy requirements.

4.2.3 Data Storage

A Safety Information System (SIS) **MAY** store DEMP data required for operation, recovery and auditability.

4.2.4 Confidentiality

A **Safety Information System (SIS) MUST** protect data exchange, data processing and data storage against unauthorized access and tampering through **documented** technical and organizational measures.

4.2.5 Autonomy

A Safety Information System (SIS) **MUST** be capable of operating autonomously within its defined scope, without requiring continuous connectivity to other Safety Information Systems or external services.

4.2.6 Deployment

A Safety Information System (SIS) **SHOULD** be deployed in a stable, managed and production-grade environment appropriate for continuous operation, scalability and appropriate levels of availability.

4.2.7 Hub

A Safety Information System (SIS) **MUST** be accessible by Entities through an access point called a **Hub**.

4.2.7.1 Interface A **Hub SHOULD** be a secure HTTP service providing web-based access to administrative information and interaction features for Entities.

4.2.7.2 Access Control Access to the **Hub MUST** be either public or private (network-restricted). It **MAY** also be subject to authentication.

4.3 Safety Zone

A **Safety Zone** (Zone) **MUST** be a defined physical or virtual area that is monitored for safety events and emergency management purposes.

4.3.1 Physical Zone

A **Physical Zone MUST** be defined by accurate **spatial references**.

4.3.1.1 Mobility A **Physical Zone MAY** be either *static* or *dynamic*, depending on whether its **spatial references** remain constant over time.

4.3.2 Virtual Zone

A **Virtual Zone MUST** be based on logical boundaries without spatial reference requirements.

4.3.3 Temporality

A **Safety Zone MAY** be defined temporarily for particular time-based events.

4.3.3.1 Time Boundaries Such zones **MUST** have explicitly defined start and end times specified in Coordinated Universal Time (UTC).

4.4 Entity

An **Entity MUST** represent a participant interacting with a Safety Information System (SIS).

4.4.1 Role

An Entity **MUST** be assigned exactly one Entity role.

4.4.1.1 Individual An Entity with this role **MUST** represent a single human person acting in an individual capacity.

4.4.1.2 Organization An Entity with this role **MUST** represent a structured group acting as a collective participant.

4.4.1.3 Autonomous Agent An Entity with this role **MUST** represent a software-based agent capable of operating autonomously and interacting with the SIS without direct human intervention.

4.4.2 Capability

An **Entity MUST** expose its technical capabilities to a **Safety Information System (SIS)**, including the actions and interactions it is able to perform within the DEMP scope.

4.4.3 Connectivity

An **Entity MUST** reflect its current connectivity state, representing its ability to establish and maintain communication with a **Safety Information System (SIS)**.

4.5 Device

A Device **MUST** be able to communicate with a Safety Information System (SIS) on behalf of an Entity.

4.5.1 Device Type

A **Device MUST** be classified as either a **Software Device** or a **Hardware Device**. This classification **SHOULD** be taken into account by interacting **Entities** to ensure correct handling.

4.5.2 Device Mode

A Device **MUST** operate in either **Active** or **Passive** mode. The selected mode defines how an Entity **MAY** interact with the Device through the Safety Information System (SIS).

4.5.2.1 Active Devices An **Active Device MAY** change its operational state in response to a request issued by an Entity.

4.5.2.2 Passive Devices A **Passive Device MUST NOT** change its operational state in response to any request issued by an Entity.

4.6 Alert

An **Alert MUST** represent a safety, security or emergency situation managed by a Safety Information System (SIS).

4.6.1 Status

Each Alert **MUST** have exactly one status that reflects its current state within the Safety Information System (SIS).

At least the following alert statuses **MUST** be defined, supported and interpreted as follows:

- **Reported**: This status **MUST** indicate that an Alert has been triggered by the Safety Information System (SIS).
- **Responding**: This status **MUST** indicate that response, coordination or mitigation actions are currently being performed.
- **Resolved**: This status **MUST** indicate that the situation has been addressed and that no further response action is required.
- **Rejected**: This status **MUST** indicate that an alert has been dismissed and **MUST NOT** require further action.

4.6.2 Level

The Alert level **MUST** indicate the escalation tier of an alert and define the expected response and handling obligations.

At least the following alert levels **MUST** be defined and interpreted as follows:

- **Test**: Alerts of this level **MUST** be used exclusively for testing or training purposes and **MUST NOT** represent real situations.
- **Information**: Alerts of this level **MUST** be intended to convey general information and **MUST NOT** require action or confirmation of reception.
- **Warning**: Alerts of this level **MUST** represent potential safety issues and **MUST** require confirmation of reception.
- **Emergency**: Alerts of this level **MUST** represent situations requiring immediate intervention.

4.6.3 Zone Alert

A **Zone Alert MUST** be generated for situations that could affect a specific physical or virtual Safety Zone within a SIS.

4.6.4 System Alert

A **System Alert MUST** be generated for situations that could affect all Safety Zones within a SIS.

4.6.5 Federated Alert

A **Federated Alert MUST** be generated for situations that could impact multiple Safety Information Systems (SIS) participating in a Federation.

4.6.6 Open Alert

An **Open Alert MUST** be generated for situations requiring widespread propagation across a DEMP Network.

4.6.6.1 Propagation An Open Alert **SHOULD** be forwarded by the originating Safety Information System (SIS) to every Federation it participates in. Each Federation member **MAY** subsequently propagate the Open Alert to third-party systems.

4.7 Federation

A Federation **MUST** be a structured group of Safety Information Systems (SIS) that voluntarily and formally collaborate through explicitly defined agreements in order to share information and, where applicable, coordinate decision-making related to safety and emergency management.

4.7.1 Structure

Federations **MAY** adopt a hierarchical structure. A hierarchical Federation **MUST** be composed of multiple federation levels, where a Safety Information System (SIS) may federate with other SIS operating at different scopes, geographical coverage, responsibilities, or jurisdictions.

4.7.2 Governance

Federation governance **MUST** be explicitly defined through formally adopted agreements and policies accepted by all participating Safety Information Systems (SIS).

4.7.2.1 Alert Management Agreement (AMA) A **Federation SHOULD** define an **Alert Management Agreement (AMA)** describing how, when and where Federated Alerts are triggered, escalated and handled across participating **Safety Information Systems (SIS)**.

4.7.2.2 Consensus Decision-Making Agreement (CDMA) A **Federation SHOULD** establish a **Consensus Decision-Making Agreement (CDMA)** that defines the applicable polling mechanisms, decision thresholds and any extended or overriding decision-making privileges.

4.7.2.3 Conflict Resolution Agreement (CRA) A **Federation SHOULD** define a **Conflict Resolution Agreement (CRA)** describing how conflicts between participating Safety Information Systems (SIS) are resolved.

4.7.2.4 Open Alert Policy (OAP) A **Federation SHOULD** establish a common **Open Alert Policy (OAP)** defining the conditions under which participating Safety Information Systems (SIS) accept, process or forward Open Alerts.

4.8 Consensus Decision-Making (CDM)

A Consensus Decision-Making (CDM) process **MAY** be used within a Safety Information System (SIS) or a Federation to resolve specific decisions.

CDM decisions **MUST** be made collectively by participating entities within the applicable scope and **MUST** be enforced by the hosting SIS or Federation in accordance with the applicable decision agreements and policies.

4.8.1 Polling

Polling is the mechanism by which participating entities express a decision within a Consensus Decision-Making (CDM) process. Polling **MUST** be bounded, deterministic and time-constrained to ensure safe and predictable outcomes.

4.8.1.1 Time-Bound Polling The polling mechanism **MAY** be time-bound to ensure prompt decision-making.

4.8.1.2 Repeated Poll A **Safety Information System (SIS) MAY** repeat a poll if the outcome cannot be formally established, provided that the conditions for such repetition are met within the applicable decision window.

4.8.1.3 Fallback Resolution If a repeated poll is not feasible due to alert level, time constraints or any other reason, the Safety Information System (SIS) **MUST** apply a deterministic fallback procedure.

The fallback procedure **MUST NOT** rely on additional polling and **MUST** produce a single, deterministic outcome.

4.8.2 Override

A Consensus Decision-Making (CDM) process **MAY** be bypassed when an Entity with sufficient privileges is available and permitted to act within the applicable scope.

5 Security and Trust

5.1 Identity

Identity defines how a Subject within the DEMP scope is uniquely identified and how control over identifiers is established and maintained over time.

5.1.1 Identifier

An Identity **MUST** be associated with one or more stable and unique identifiers within the DEMP Network scope.

5.1.2 Binding

Identity binding methods **MUST** define how an identifier is initially assigned to a Subject and how this association is established as authoritative within a defined scope.

Binding **MUST** be explicit and auditable and **MUST NOT** imply global authority or transitive trust.

At least the following identity binding methods **SHOULD** be supported.

5.1.2.1 Trust-On-First-Use (TOFU) Under the Trust-On-First-Use (TOFU) binding method, an identifier **MUST** be accepted on its first encounter and **MUST** be considered trusted as long as continuity is maintained.

5.1.2.2 Explicit Binding Under the Explicit Binding method, an identifier **MUST** be bound through an explicit and trusted verification process.

5.1.2.3 Delegated Binding Under the Delegated Binding method, an identifier **MUST** be bound through delegation by another trusted party.

5.1.2.4 Self-Asserted Binding Under the Self-Asserted Binding method, an identifier **MAY** be claimed without prior verification and **MUST** be treated as unverified.

5.2 Authentication

Authentication **MUST** be the mechanism by which an Entity proves control over its Identity to a Safety Information System (SIS), or by which an SIS proves control over its Identity to a Federation.

5.3 Certification

Certification **MUST** establish *verifiable trust claims* that can be independently validated through a Chain of Trust.

5.3.1 Authority

A **Certification Authority MUST** be an independent organization responsible for evaluating and certifying Entities, Safety Information Systems and Federations in accordance with the applicable Certification Framework.

A Certification Authority:

- **MUST** be organizationally and operationally independent from the subject it certifies
- **MUST** apply evaluation criteria that are publicly available
- **MUST** apply evaluation criteria consistently to all subjects it certifies
- **MUST** be clearly identifiable and accountable

- **MUST** support certification lifecycle management, including issuance, expiry, suspension and revocation

5.3.1.1 Oversight Certification Authorities **MAY** perform peer oversight to assess compliance with this specification and adherence to recognized best practices.

5.3.2 Framework

Any certification issued under the Certification Framework:

- **MUST** be issued by a Certification Authority
- **MUST** be unambiguously attributable to a specific Certification Authority
- **MUST** be time-bounded, with an explicit validity period
- **MUST** support suspension and revocation
- **MUST** be cryptographically verifiable

5.4 Authorization

Authorization **MUST** define a privileges-based model governing the permission to perform actions by Entities, Safety Information Systems (SIS), and Federations within the DEMP scope.

5.5 Auditability

Trust-related events **MUST** be auditable.

Auditability **MUST** allow independent verification that trust-related lifecycle events occurred, were not altered, removed or suppressed.

5.5.1 Pseudonymity

Audit records **MUST** be pseudonymous by design.

5.5.2 Registry

To support immutability and non-repudiation, trust-related lifecycle events **MUST** be recorded in an append-only audit registry.

6 Accessibility

Implementations **MUST** ensure that alerts and other safety-critical information remain accessible to all users, regardless of physical, sensory, cognitive or situational limitations.

6.1 Inclusion

Implementations **MUST** provide an inclusive user experience enabling access for users with disabilities, including but not limited to visual, auditory, motor and cognitive impairments.

6.2 Adaptability

Implementations **MUST** be designed to operate effectively under adverse conditions commonly associated with emergency situations and **SHOULD** optimize resource usage to minimize computational load, network bandwidth and energy consumption.

6.3 Internationalization

Alerts and generic emergency instructions **MUST** be expressed in a language-agnostic form at the protocol level, enabling localized rendering by implementations without altering the underlying semantic meaning.