DEMP Specification

DEMP-SPEC 0.2.0

Revision history:
https://demp.ch/spec/CHANGELOG.md

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.

1 Scope

The **Decentralized Emergency Management Protocol (DEMP)** ensures secure, interoperable and decentralized communication between Safety Information Systems (SIS), whether operating as standalone instances or within a federated network. It facilitates real-time data exchange across safety zones, entities, and devices, enabling seamless coordination and an effective, community-driven and digitally enhanced response during emergencies.

The **Decentralized Emergency Management Protocol Specification (DEMP-SPEC)** defines a technical standard that outlines a framework and guidelines for implementing and interacting with decentralized emergency management systems.

The primary goal of this specification is to provide comprehensive documentation for developers and integrators, enabling them to create or integrate DEMP-based systems and applications. It describes the components, rules, and data structures necessary for the successful deployment of safety information systems in various environments.

It is important to note that this specification does not address the organization or operational implementation of Safety Information Systems (SIS), nor does it cover the detailed design of software or hardware devices.

2 Audience

The specification is intended for a variety of stakeholders involved in the development, integration, and operation of decentralized emergency management systems. The primary audience includes:

- **System Architects and Developers**: Those designing and developing DEMP-compliant software.
- **Integrators**: Professionals responsible for integrating DEMP-compliant solutions.
- **Device Manufacturers**: Organizations that produce DEMP-compliant devices and software.
- **Security and Safety Specialists**: Professionals involved in emergency management.
- **Cybersecurity Specialists**: Professionals involved information security and cyber risk management.
- **Lawyers**: Legal professionals ensuring that DEMP complies with relevant laws and regulations.
- **Policy Makers and Regulators**: Authorities responsible for regulating emergency management systems.
- **Volunteers**: Individuals and communities actively promoting the adoption and implementation of DEMP.

3 Versioning

The document follows **Semantic Versioning (SemVer) v2.0.0** to manage its releases and updates. This approach ensures that developers and integrators can understand the impact of each version based on the changes made in the specification.

4 Contributors

- **Jean-Pierre Grossglauser**: Lead Author, Software Developer

5 Components

5.1 DEMP Network

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

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

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

5.1.4 Communication A DEMP Network **SHOULD** be based on Internet Protocol (IP) for communication and Domain Name System (DNS) for naming and addressing purposes.

Communication channels **MUST** be encrypted using appropriate cryptographic means.

5.1.4 Data Exchange A DEMP Network **SHOULD** facilitate efficient data exchange between connected Safety Information Systems (SIS) in terms of latency, bandwidth usage and availability.

5.1.5 Scalability A DEMP Network **MUST** be designed to scale, meaning new Safety Information System (SIS) **MUST** be able to be added seamlessly and SIS **MUST** be able to be removed without impacting the overall network's operations or availability.

5.1.6 Wide Area Network (WAN) A DEMP Network **SHOULD** be accessible across the Internet Wide Area Network (WAN) and this network **SHOULD** be referred to as the **Global DEMP Network**.

5.1.7 Local Area Network (LAN) A DEMP Network **SHOULD BE** able to function as Local Area Network (LAN), with Safety Information Systems (SIS) that are not reachable beyond those network boundaries.

5.1.8 Virtual Private Network (VPN) A DEMP Network **SHOULD BE** able to function as Virtual Private Network (VPN), with Safety Information Systems (SIS) that are not reachable beyond those network boundaries.

5.1.9 Ad Hoc Network A Safety Information System (SIS) **MAY** support operation within a local mesh or peer-to-peer (P2P) ad hoc network that enables offline or short-range data exchange with participating Entities. In this mode, DEMP messages **SHOULD** be transmitted over any compatible communication protocol that supports secure, multi-hop or direct message propagation.

5.1.10 Network Directory A **Network Directory MUST** provide an up-to-date registry of all participating **Safety Information Systems (SIS)** within a DEMP Network. Each SIS **MUST** be able to access that directory and opt-in or opt-out as needed.

5.2 Safety Information Systems (SIS)

A **Safety Information System (SIS)** is designed to monitor, manage, process, and exchange safety-related data across entities, devices, and other SIS, either as a standalone server instance or by joining a decentralized network (see **Federation**).

For production use, an SIS **should** be deployed as a network device, as a router service, or as a cloud service.

Any custom device or improvised hosting setup **must** be limited to test and development environments only.

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

A **Hub SHOULD** be an HTTP service serving web pages with administrative information and features for entities to interact with the SIS.

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

5.2.2 Certified Safety Information System (SIS) A **Certified Safety Information System (SIS) SHOULD** undergo a formal certification process to confirm that it complies with established security, operational, and legal requirements. The certification process **MUST** ensure that the system meets predefined standards for data privacy, integrity, safety, and governance, as well as compliance with relevant local or international regulations.

5.3 Safety Zones

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

5.3.1 Physical Zones A **Physical Zone MUST** be defined by accurately mapped geospatial data.

5.3.2 Virtual Zones A **Virtual Zone MUST** be based on logical boundaries without geospatial data requirements.

5.3.3 Temporality A **Safety Zone MAY** be defined temporarily for particular time-based events. Such zones **MUST** have start and end times specified in UTC time.

5.4 Entities

An **Entity** in DEMP **MUST** represent an individual, organization, or autonomous agent interacting with a Safety Information System (SIS).

5.4.1 Roles An **Entity MUST** have one of the following roles: - **Individual**: A person. - **Organization**: A group of persons. - **Autonomous Agent**: A software able to run automated tasks and make decisions without human action.

5.4.2 Authentication An **Entity MUST** be uniquely identified within the SIS.

5.4.3 Identification An **Entity MUST** authenticate to the SIS before any interaction or action can be performed.

5.4.3.1 Individuals Entities with the **Individual** role **MUST** use 2-factor authentication, where one of the factors **MUST** be biometric.

5.4.3.2 Organizations Entities with the **Organization** role **MUST** use cryptographic authentication.

5.4.3.3 Autonomous Agents Entities with the **Autonomous Agent** role **MUST** use cryptographic authentication.

5.4.4 Managed Entities A Managed Entity **MUST** be under the full control of an SIS and **SHOULD** usually involve an Autonomous Agent Entity with a Software Device.

5.4.5 Certified Entities A **Certified Entity MUST** have successfully completed an administrative and technical identity validation process, confirming its authenticity within an SIS. This certification **MUST** ensure that the entity meets specific security, operational, and legal requirements.

5.4.6 Authoritative Entities An **Authoritative Entity MUST** be a Certified Entity that has successfully completed an extended administrative and legal verification process to obtain elevated management privileges within a Safety Information System (SIS).

An **Authoritative Entity**, upon acquiring elevated management privileges, **MUST** be legally accountable for the use of those privileges.

5.5 Devices

Devices MUST be able to share or exchange data with a Safety Information System (SIS) on behalf of an Entity.

5.5.1 Device Types A Device **MUST** be classified as either a **Software** or **Hardware** device. This classification **SHOULD BE** considered by a Safety Information System (SIS) to ensure proper interaction.

5.5.2 Device Modes Devices **MUST** operate either in Active or Passive mode. Each mode dictates the level of interaction the device can have with the SIS.

5.5.2.1 Active Devices **Active Devices MUST** be able to both send and receive data from the Safety Information System (SIS). These devices **MAY** receive push operations from an SIS Managed Entity, and the SIS Managed Entity **MAY** also initiate pull operations to retrieve data from these devices. Active devices **MUST** support both the push and pull operations.

5.5.2.2 Passive Devices **Passive Devices MUST** be able to share data with the Safety Information System (SIS), but they **MUST NOT** initiate communication themselves. Instead, an SIS Managed Entity **MUST** use pull operations to retrieve data from passive devices. These devices **MUST** only respond to pull requests from the SIS they belong to.

5.6 Alerts

An **Alert MUST** be a real-time message sent by the Safety Information System (SIS) in response to particular events or conditions originating from any Entity activity.

5.6.1 Alert Status Each alert **MUST** have a status that reflects its current state within the SIS. At least the following statuses **MUST** be defined: - **Triggered**: The alert has been raised but no action has been taken. - **In Progress**: The alert is being actively managed. - **Resolved**: The alert has been addressed and no further action is required. - **Cancelled**: The alert was dismissed or deemed unnecessary.

Any additional alert statuses **SHOULD** be implemented in such a way that they do not break compatibility and interoperability across Safety Information Systems (SIS).

5.6.2 Alert Severity **Alert Severity MUST** categorize alerts based on their severity to prioritize responses. At least the following severity levels must be defined:

- **Test**: Alerts that are used for testing or validation purposes and should not be treated as real emergencies.
- **Information**: Low-priority alerts that provide general information.
- **Warning**: Alerts that indicate potential issues that need attention but do not require immediate action.
- **High**: Alerts that represent significant concerns requiring immediate attention and action.
- **Critical**: Alerts representing a critical emergency situation requiring urgent action.

Any additional alert severities **MUST** be implemented in such a way that they do not break compatibility and interoperability across Safety Information Systems (SIS).

5.6.3 Zone Alert A **Zone Alert MUST** be generated for events that could affect a specific physical or virtual safety zone within a SIS. Zone alerts **MUST** apply to any entities within the zone that are either actively or passively impacted by the event.

5.6.4 System Alert A **System Alert MUST** be generated for events that could affect all Safety Zones within a Safety Information System (SIS). This alert **MUST** apply to all entities from all Safety Zones within the SIS.

5.6.5 Federated Alert A **Federated Alert MUST** be generated for events that could impact multiple Safety Information Systems (SIS) participating in a Federation. A Federated Alert **MUST** be forwarded to every SIS in the Federation as a **System Alert**.

5.6.6 Open Alert An **Open Alert MUST** be generated for events that would require widespread propagation across an entire DEMP Network. This type of alert **MUST** attempt to reach all Safety Information Systems (SIS) within the network, beyond just the federated SIS nodes.

5.6.6.1 Propagation An **Open Alert MUST** be forwarded to every Federation a SIS is a member of. Every Federated SIS **SHOULD** then propagate the alert according to the Federation's Open Alert Policy, and third-party SIS **MAY** forward it beyond the Federations they are a member of, according to their respective policies.

5.7 Federations

A **Federation MUST** be a group of Safety Information Systems (SIS) that collaborate to exchange data and coordinate emergency management during widespread alerts.

5.7.1 Federation Structure Federations **SHOULD** adopt a **Hierarchical Federation** structure.

A **Hierarchical Federation MUST** consist of multiple levels, where a Safety Information System (SIS) is a member of a federation that is part of a larger federation, which **SHOULD** be organized based on geographical and organizational criteria.

Hierarchical Federations MUST not impose authority or a decision-making process beyond the scope of the federation itself.

5.7.2 Accountability Framework The **Federation MUST** establish an Accountability Framework to ensure that each member Safety Information System (SIS) owner and/or representative understands roles, processes, and responsibilities.

5.7.3 Alert Management Agreement (AMA) The **Federation MUST** define an Alert Management Agreement (AMA) for managing alerts across all members. This process **MUST** ensure that Federated Alerts are triggered, escalated, and handled in a coordinated and common manner for every concerned Safety Information System (SIS).

5.7.4 Consensus Decision-Making Agreement (CDMA) The **Federation MUST** establish a Consensus Decision-Making Agreement (CDMA) that outlines the voting process and authoritative entity privileges.

5.7.5 Conflict Resolution Agreement (CRA) The **Federation MUST** define a Conflict Resolution Agreement (CRA) that defines the process used to resolve disagreements between members. This process **MUST** ensure that disputes cannot critically disrupt Safety Information Systems (SIS) operations in case of ongoing emergencies.

5.7.6 Open Alert Policy (OAP) The **Federation SHOULD** establish a common **Open Alert Policy** (OAP) that defines the conditions under which members **SHOULD** handle **Open Alerts**. The policy **MUST** ensure consistent processing of **Open Alerts** across all Safety Information Systems (SIS) within the Federation.

5.8 Consensus Decision-Making

The consensus decision-making process **MUST** involve a polling mechanism to ensure that all participating entities within a Safety Information System (SIS) or a Federation reach a unified agreement before taking significant decisions.

5.8.1 Discussions Prior to Polling The polling mechanism **MAY** be preceded by discussions between entities. These discussions provide a transparent space for deliberation before the formal poll.

5.8.2 Time-Bound Polling The polling mechanism **MAY** be time-bound to ensure prompt decision-making, which is essential during emergency situations to minimize delays.

5.8.3 Weighted Voting Mechanism Entities may have greater influence based on their role, authority, or responsibility within the Safety Zone or Safety Information System (SIS). These weights **MUST** be defined within the Safety Information System (SIS) prior to any emergency event.

5.8.4 Authoritative Entity Override The polling mechanism **MAY** be bypassed by any available **Authoritative Entity**, provided that such a privilege is part of a Safety Information System (SIS) or Federation pre-established agreement.

5.8.5 Tie-Breaking Mechanism If a Tie-Breaking Agreement hasn't been pre-established at the Safety Information System (SIS) or Federation level, one or more of the following mechanisms **SHOULD BE** implemented:

- The decision **SHOULD BE** delegated to any available **Authoritative Entity**.
- The poll **MAY** be repeated if alert severity is not considered as critical.

5.9 Chain of Trust

A **Chain of Trust MUST** be established to ensure that all information exchanged across Safety Information Systems (SIS), devices, and entities is authentic, secure, and tamper-proof. This Chain of Trust **MUST** be built using cryptographic techniques, validation mechanisms, and certificates that establish trust between entities participating in a DEMP Network.