Velsanet City-level E2E Management Center White Paper

Draft v1.0 — Structure and Design Specification

1. Introduction

1.1 Background and Motivation

Urban life increasingly depends on continuous connectivity among households, sensors, robotics, transportation systems, and public services. However, existing Internet and telecom structures are optimized for best-effort packet delivery and commercial service bundling—not for accountable public safety operations.

1.2 Limitations of Existing ISP- and Platform-Centric Models

- Fragmented responsibility across ISPs, platforms, and municipal agencies.
- Weak linkage between city operations and household-level emergency endpoints.
- Privacy handled by policy and contracts rather than by structural separation.
- Centralized cloud dependencies and slow emergency coordination under failure.

1.3 Purpose of the City-level E2E Management Center

This white paper defines the architecture of a Velsanet-based City-level End-to-End (E2E) Management Center: a public infrastructure node that integrates city governance functions with ISP-equivalent operational domains through structurally separated E2E channels.

1.4 Scope of This White Paper and Future Updates

This white paper defines the core architectural principles, structural boundaries, and operational framework of the City-level E2E Management Center. Domain-specific accommodation methods—such as transportation, energy, environment, or other public services—are intentionally not exhaustively specified in this initial draft. These methods will be incrementally defined and updated based on the characteristics and requirements of each domain, while remaining consistent with the architectural principles established herein.

2. Concept of E2E-Native Urban Infrastructure

2.1 End-to-End as a Structural Principle

In this document, E2E refers to structurally preserved connectivity and responsibility boundaries from endpoints to the responsible public operator, not merely an application-layer secure session.

2.2 Public vs. Private Domains in E2E Architecture

Velsanet separates public-domain connectivity and private-domain connectivity at the physical and logical boundary. Public channels serve safety and governance functions; private channels serve optional personal or service-specific functions. This separation is structural, not policy-based.

2.3 Why Cities Require E2E Management Centers

Cities need an accountable E2E operator that can coordinate safety, emergency communications, and public broadcasting under failure and scale. The City-level E2E Management Center provides this role as a stable, auditable public infrastructure component.

3. Scope of Authority and Responsibility

3.1 Government and Municipal Roles

- Public safety: fire response, policing coordination, emergency guidance.
- Disaster response: alerts, evacuation coordination, continuity of operations.
- Public communications: citywide broadcasting and verified public messaging.
- Urban operations: aggregated state signals from public endpoints and infrastructure.

3.2 Structural Inclusion of ISP Functional Domains

The Center structurally includes core ISP-equivalent domains—telephony, broadcasting delivery coordination, security monitoring linkage, and network operations—not as commercial bundles, but as accountable public capabilities.

3.3 Responsibility, Accountability, and Governance Boundaries

The Center is responsible for public-domain channels only. It does not operate as a general-purpose surveillance system and cannot access private domains under normal conditions. Accountability is enforced via role-based access controls, logging, and post-incident audits.

4. Home-level Public E2E Connection Architecture

4.1 Home-level Public E2E Access Unit

Each household is equipped with a dedicated Home-level Public E2E Access Unit that defines the minimum structural boundary between private living space and city-level public

infrastructure. The unit performs no computation and stores no personal content; it provides deterministic connectivity boundaries.

4.2 Dual Optical Core Structure

- Public Optical Core: reserved exclusively for public E2E connectivity to the City-level E2E Management Center.
- Private/Optional Optical Core: allocated for optional private or service-specific connectivity and remains structurally isolated from public channels.

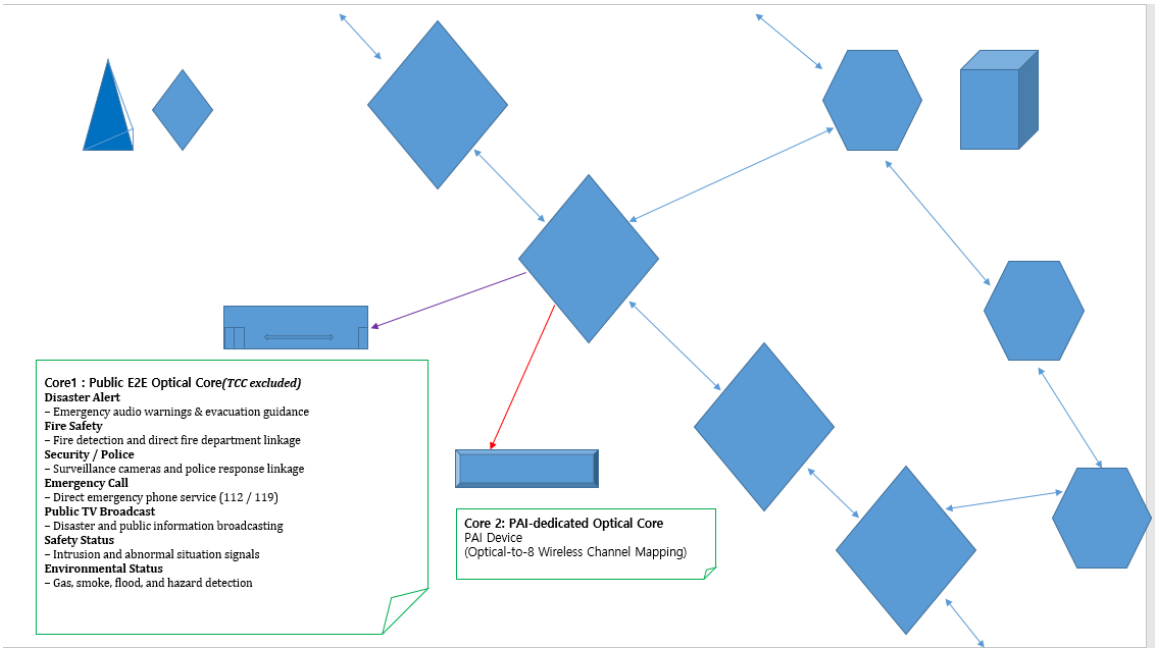

Figure 4.2 Home-level Dual Optical Core Architecture with Public E2E and PAI Connectivity

This figure illustrates the home-level connection architecture in the Velsanet system, where each household is provisioned with ***two physically and logically independent optical cores****.*

The ***first optical core (Public E2E Optical Core)*** *is exclusively reserved for public-domain end-to-end connectivity.*
It directly links the household to the City-level E2E Management Center and supports seven parallel Public E2E channels, including disaster alerts, fire safety, emergency calls, public broadcasting, security linkage, and environmental status signaling.
These channels operate independently and remain structurally isolated from private services, ensuring predictable behavior and continuity during emergency conditions.

The ***second optical core (PAI-dedicated Optical Core)*** *is allocated exclusively for Personal AI (PAI) connectivity.*
This core terminates at a dedicated PAI device within the household, where a single optical link is mapped to ***eight independent wireless channels****.*

Through this optical-to-multi-wireless channel mapping, the PAI directly manages multiple personal devices, sensors, and interfaces without traversing public E2E channels or ISP-managed service layers.

By separating public E2E connectivity and PAI connectivity at the optical core level, the architecture establishes a ***clear structural boundary between public responsibility and personal AI sovereignty****.*
This design ensures that public safety operations, private life, and personal AI systems coexist within the same household without functional overlap, policy-based dependency, or implicit access paths.

4.3 Public Optical Core and Channel Separation

Within the public optical core, seven dedicated public channels operate in parallel and remain mutually isolated to contain faults and prevent cross-domain leakage.

4.4 Position of the Household as a Public Infrastructure Endpoint

In Velsanet, the household is not defined primarily as an Internet service consumer. It is a protected endpoint of the city's public safety and governance infrastructure with structurally bounded interfaces.

4.5 Shared Wireless Domain for PAI Connectivity

To support continuous Personal AI (PAI) connectivity across multiple physical spaces within a household, the Velsanet architecture introduces the concept of a **Shared Wireless Domain (SWD)**.

A typical household consists of multiple spatial zones—such as living rooms, bedrooms, kitchens, and workspaces—where PAI-managed devices, sensors, and interfaces may operate concurrently.
In such environments, independent or access-point–centric wireless connections are insufficient to preserve continuity of PAI operation.

4.5.1 PAI Wireless Domain Anchor

The PAI-dedicated optical core terminates at a single **PAI Device**, which acts as the **Wireless Domain Anchor**.

This anchor:

- Maintains identity, policy, and session continuity for all PAI-managed devices
- Serves as the sole control and coordination point for the wireless domain
- Prevents fragmentation of PAI state across multiple access points

4.5.2 Distributed Wireless Extension Nodes

Within the household, multiple lightweight wireless nodes may be deployed to extend coverage across physical spaces.

These nodes:

- Perform radio transmission and reception only
- Do not implement independent authentication, policy, or intelligence
- Operate as extensions of the PAI Wireless Domain Anchor

From the perspective of PAI-managed devices, these nodes collectively form **a single logical wireless domain**, not separate access points.

4.5.3 Continuous Connectivity Model

Under the Shared Wireless Domain model:

- Devices move within the household without session termination
- No access-point switching or re-authentication is required
- Wireless continuity is preserved as a property of the PAI domain, not the radio endpoint

This ensures uninterrupted interaction between PAI and its associated devices, regardless of physical movement within the home.

4.5.4 Architectural Distinction

The Shared Wireless Domain differs fundamentally from traditional Wi-Fi mesh or roaming systems.

- Control is **PAI-centric**, not access-point–centric
- Identity and policy remain anchored at the PAI device
- Wireless nodes are structurally subordinate extensions, not autonomous network elements

This distinction is essential for maintaining PAI sovereignty and preventing implicit dependency on ISP-managed or platform-controlled wireless infrastructures.

4.5.5 Role within the Home-level Dual Optical Core Architecture

The Shared Wireless Domain operates exclusively over the **PAI-dedicated optical core** and remains completely isolated from Public E2E channels.

This design guarantees that:

- Public safety and governance operations do not interfere with PAI connectivity
- PAI wireless operations cannot be observed or influenced by public-domain systems
- Personal AI sovereignty is preserved at both optical and wireless layers

5. Public E2E Channel Control Zone

5.1 Role of the Public E2E Channel Control Zone

The Public E2E Channel Control Zone is the operational domain responsible for managing the public channels, enforcing isolation, and ensuring emergency continuity.

This section defines the maximum scope of city-level authority within the Velsanet architecture.

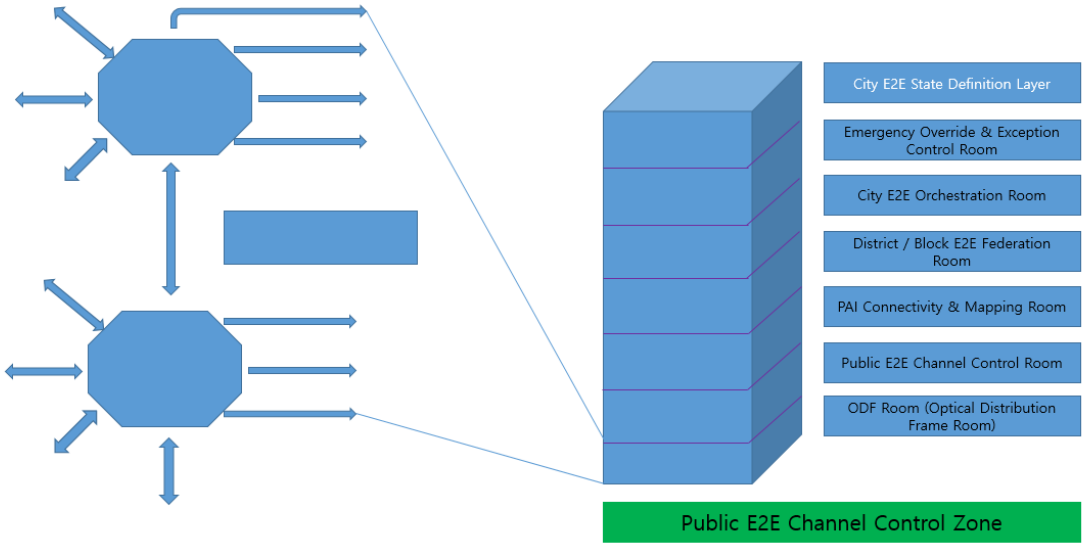

Figure 5-1. Layered Architecture of the City-level E2E Management Center

This figure presents the City-level E2E Management Center as a vertically layered architecture in which each layer has a clearly defined scope, authority, and operational boundary.

Lower layers are responsible for physical optical connectivity and public E2E channel control, while intermediate layers manage personal AI (PAI) connectivity, shared wireless domain mapping, and district-level federation within the city. Upper layers coordinate city-wide E2E orchestration and handle emergency exception mechanisms.

At the top of the architecture, the City E2E State Definition Layer defines the operational state of public E2E infrastructure without directly controlling lower-layer operations. Crucially, this layer explicitly excludes Personal AI (PAI) domains from state definition or evaluation, ensuring structural separation between public governance and personal AI sovereignty under all operational conditions.

5.2 Definition of the Seven Public E2E Channels

- Disaster Alert — Emergency audio warnings and evacuation guidance (speaker).
- Fire Safety — Fire detection and direct fire department linkage.
- Security / Police — Surveillance camera linkage for emergency response.
- Emergency Call — Direct emergency phone services (e.g., emergency numbers).
- Public TV Broadcast — Disaster and public information broadcasting.
- Safety Status — Intrusion and abnormal situation signals.
- Environmental Status — Gas, smoke, flood, and hazard detection.

5.3 Channel Isolation and Parallel Operation

- Parallel operation prevents single-channel overload from cascading across channels.
- Isolation enables predictable emergency behavior and faster fault localization.
- Channel-level policies define what is transmitted: primarily state, event, and response signals.

5.4 Integration with City-level E2E Management Center

Public channels terminate at the City-level Center through the Optical Core Termination and ODF domains, where control and emergency operations coordinate responses.

6. City-level E2E Management Center Architecture

6.1 Core Functional Components

- Public E2E Channel Control Zone (operational control).
- Emergency Operations Zone (incident response and escalation).
- Monitoring & Telemetry Zone (public-domain state/event aggregation).
- Governance & Audit Zone (policy enforcement, logging, review).
- Inter-Center Coordination (district/neighborhood and peer-city links).

6.2 Optical Core Termination and ODF Structure

The Center includes an Optical Distribution Frame (ODF) Room for optical core termination, patching, and structured expansion. This physical separation supports incremental capacity growth and fault isolation.

6.3 Control, Monitoring, and Emergency Operations

Operational control manages channel integrity and routing within the public domain. Emergency operations coordinate rapid response actions with municipal agencies and verified broadcast mechanisms.

6.4 Replacement of Legacy NOC and ISP Operations

Traditional ISP NOC functions are transformed into public-domain E2E operations: channel continuity, fault localization, prioritized emergency handling, and structured scaling—without commercial bundling assumptions.

7. Information Handling and Access Control

7.1 Structurally Restricted Access Model

Under normal conditions, the Center handles public-domain state and event information only. Private domains remain structurally inaccessible by default.

7.2 Role-Based and Channel-Based Information Handling

- Role-based access: operators see only what their operational role requires.
- Channel-based handling: each channel defines permissible payload types and actions.
- Minimization: prefer state/event signals over raw personal content.

7.3 Logging, Auditability, and Transparency

All operational actions affecting public channels are logged. Logs enable audits, incident reconstruction, and accountability reviews without requiring routine access to private domains.

8. Emergency Override Principle

8.1 Definition of Emergency Conditions

- Life-threatening events (fire, severe injury, imminent harm).
- Large-scale disaster conditions (earthquake, flood, severe weather).
- Critical infrastructure failures affecting public safety.

8.2 Exception-Based Access Rules

Emergency override allows limited access only when necessary to protect life and safety. Overrides are exception-based, not continuous privileges.

8.3 Temporal and Functional Limitation of Overrides

- Time-bounded: automatically expires after the emergency window.
- Scope-bounded: limited to relevant channels and endpoints.
- Function-bounded: limited to actions required for emergency response.

8.4 Post-Incident Review and Accountability

All overrides are recorded and subject to post-incident review. Governance processes validate necessity and prevent abuse.

9. Multi-Scale E2E Management and Urban Scaling

9.1 Neighborhood-level E2E Nodes

Neighborhood-level nodes provide local aggregation of public channels, first-response coordination, and rapid fault containment within daily living zones.

9.2 District-level E2E Centers

District-level centers coordinate among multiple neighborhood nodes, provide load redistribution, and isolate localized failures from wider city impact.

9.3 City-level E2E Management Center

The city-level center provides citywide orchestration, verified public communications, and final accountability for public-domain E2E operations.

9.4 Peer-Managing and Hierarchical Coordination

- Hierarchical escalation for accountability and large-scale coordination.
- Peer coordination between units for rapid rerouting and localized response.
- Autonomy at each level to maintain continuity when higher levels are degraded.

10. Resilience, Fault Isolation, and Continuity

10.1 Independent Operation Across Scales

Each scale unit can maintain essential public services during partial failures, with graceful degradation rather than system-wide collapse.

10.2 Load Redistribution and Failover

Parallel channels and multi-level centers enable rerouting and load balancing under congestion, physical damage, or localized outages.

10.3 Disaster-Scale Structural Stability

The structure prioritizes safety and continuity under disaster conditions by design: isolation, deterministic control, and auditable emergency privileges.

11. Impact on Urban Governance and Industry

11.1 Transformation of Public Safety and Disaster Response

Public channels become a continuously connected, E2E-native safety fabric linking households and urban operators with reduced latency and clearer accountability.

11.2 Structural Supersession of ISP Business Models

Commercial ISP bundles become optional overlays rather than the core operating model. Public telephony, broadcasting, and safety operations are structurally integrated within the city's E2E infrastructure.

11.3 Implications for Smart Cities and Future Urban Systems

The Center provides a stable foundation for robotics, V2X, sensors, and future urban automation by enforcing structural boundaries between public responsibility and private life.

12. Conclusion

12.1 Summary of Architectural Advantages

- Structural separation of public and private domains at the household boundary.
- Seven parallel public safety channels managed as public infrastructure.
- Auditable emergency override rather than continuous surveillance.
- Multi-scale scaling across neighborhood, district, and city levels.
- Capacity growth through ODF-based optical core expansion and fault isolation.

12.2 City-level E2E Management Center as Urban Infrastructure

The City-level E2E Management Center is positioned as an essential public infrastructure component—an accountable operator of public-domain E2E connectivity, not a commercial service provider.

12.3 Path Toward Global Adoption

Because the architecture is defined by functional scales (neighborhood, district, city) rather than local administrative terminology, it can be adopted globally while respecting regional governance structures and legal frameworks.