ZPR Terminology

Dave Douglas, Frank Kastenholtz, Steve Willis, September 2020
(Updated August 28, 2025)

1. Introduction

This document defines terms used when discussing ZPR and its various components.

2. ZPR Glossary

Term	Definition
Adapter	Software that allows standard IP-based applications to connect to a ZPRnet through a secure docking session.
Assertion	A declarative statement of policy intent in ZPL used to ensure permissions align with intended security goals and do not permit unintended communication.
Attribute	A property of an identity (user, device, or service); may be a tag, a name/value pair, or a name/multi-value set.
Authentication	The process of verifying the association between an identity and its device, user, or service.
Authentication Service	A service that validates the identities of endpoints, users, or services; multiple may exist in ZPRnet.
Byzantine Fault Tolerance	A method of building fault-tolerant services that can withstand component failures or compromises.
Certificate	A cryptographic document proving the association of a service identity with a specific endpoint and ports.
Circumstance	A runtime condition (e.g., time of day, data volume, recent usage) that can influence permissions.
Class	A defined group of entities (e.g., users, services) with shared attributes; can be subclassed.
Compliant Flow	A secure, policy-compliant communication path between endpoints, guided by visas.
Configuration	A complete, testable set of policies and network settings that define how ZPRnet operates.
Configuration Description	A ZPL component defining network-specific settings such as topology and IP addresses.
Device Identity	An identity for a device, typically associated with a MAC address, TPM, or certificate.
Dock	An interface on a node that connects to endpoints using IP protocols.
Endpoint	The device or interface that connects ZPR protocols to standard IP protocols or to ZPRnet (e.g., NIC, adapter); may be virtual or physical.
Flow	A unidirectional communication stream between endpoints, which may be governed by policies based on identity.

Term	Definition
Identity	A unique key used to retrieve attributes associated with an endpoint, user, or service.
Identity Attribute	A specific attribute value, such as a serial number, used to validate an identity association.
Incremental Compilation	The ability to independently compile and combine parts of policy for modular policy management.
Management Packet	An internal packet used for control-plane functions such as visa distribution.
MICV	Message Integrity Check Value; a cryptographic hash ensuring the integrity of a transit packet.
Multiple Names	User or service identities may be mapped from multiple names to a single identity.
Multiple Users per Endpoint	A condition where a device hosts more than one user; packet flow may be user-agnostic.
Name	A string used for identifying attributes, identities, or classes; may include a namespace prefix.
Namespace	A context in which names are defined; names in different namespaces are not equivalent.
Node	A ZPR component that forwards packets and enforces policy.
Paranoid Design Principles	Four core security principles underlying ZPR's trust-minimized network design.
Permission	A positive policy statement in ZPL that allows communication under certain attribute-based conditions and circumstances.
Port Attribute	An attribute of a service identity indicating the ports on which it communicates.
Service	An application that sends/receives packets; has an identity and attributes, and is bound to endpoints by port.
Service Identity	An identity for a service, authenticated through certificates and tied to port numbers.
Signal	A message triggered by a matching policy statement to notify another service (e.g., a logger).
Statement	A line of ZPL code defining permissions, assertions, class definitions, or other policy elements.
Tag	An attribute with a name but no associated value.
Transit Packet	An internal ZPR packet that carries data using a visa identifier instead of IP addresses.
Trusted Source	A verified system (e.g., LDAP, Active Directory) used to retrieve attribute values.
User	A person or authority with an identity and attributes; can be associated with a flow through an endpoint.
User Identity	An identity tied to a user, usually authenticated via credentials such as passwords or certificates.
Visa	A cryptographic certificate authorizing packet travel; defines authentication, permissions, and routing.
ZDP	ZPR Data Protocol; allows secure tunnels through IP networks to connect adapters with docks.

Term	Definition
ZPL	Zero-Trust Policy Language; a human-readable language used to define, audit, and enforce communication policies in ZPRnet, including permissions, assertions, and class definitions.
ZPL Compiler	The component that checks consistency of permissions and assertions and generates enforcement rules.
ZPR	Zero-Trust Packet Routing; a network architecture that enforces communication policies within the network.
ZPR Endpoint	A user, device, or service with an authenticated identity participating in communication via ZPRnet.
ZPRnet	A network or group of interconnected ZPR nodes that enforce communication policies using visas, compliant flows, and ZPL rules.

3. Revision History

1. Revision as of August 28, 2025

    1.1 Updated list of terms