Kentucky Department of EDUCATION

Office of Education Technology

KETS Telecommunication Connectivity Standard

Version 1.2 – 03/06/2024

Document Owner:	Paul Shoemaker	Date Created:	2/8/2023
Approver:	OET Leadership	Date Approved:	4/17/2024

Summary: This document will provide the requirements and recommendations for the installation and general deployment of voice-related connectivity for Kentucky K-12 School Districts, including voice services, POTS replacement and failover voice systems. This document should be shared with vendors, so they will understand these requirements prior to offering solutions. The goal is to assist in creating solutions that best serve the district and meet all necessary security and connectivity requirements before financial obligations are established or installation activity begins. KDE strongly recommends that districts have a potential vendor perform a proof of concept within the district's environment prior to purchase (i.e., try before you buy).

Intended Audience: The audience of this technical guide is District EdTech Staff, vendors/service providers, OET Operational Support Staff, and KETS Engineers (KETS Field Staff). This document is to be shared within this audience to establish needs of the districts and ensure the solutions will operate within the technical and security requirements of the KETS environment.

Purpose and Scope: KDE/OET administers and maintains the district KETS environment of shared services. These include Internet connectivity and the security related to those services. Due to new concerns, Cyber Insurance for example, KDE/OET retains a security profile to provide a secure network environment for all Kentucky K-12 School Districts. Any solutions connecting and/or using the KETS network will be required to follow the security requirements developed by KDE/OET.

Reason for Implementing: Voice and related services can be challenging to implement in a complex, security-focused network, and establishing clear technical standards should reduce these challenges.

I. I.P. Addressing Requirements

A. The vendor/vendor partner must control the outbound destination IP addresses or domains used by the service.

B. The vendor/vendor partner must own or lease the range of IP Addresses.

1. An "open" range of rotational IP addresses shared with other services are not permitted, especially if leased from a source like AWS (Amazon Web Services) or Akamai (as examples).
2. For the outbound destination IP addresses please note if it is the vendor or vendor partner who owns the ranges.
3. Domains will need to be resolved via reverse DNS. For the outbound destination domains please note if it is the vendor or vendor partner who owns the domains.

4. Inbound access from “ANY” to any internal IP range will not be allowed. This cannot be allowed and will not work within the KETS security environment.
5. For a specific Network Address Translated (NAT) destination it will be restricted to a single NAT IP Address destination within that district’s internal network.

II. TCP/UDP Port Restrictions

A. It is strongly recommended that as few inbound ports be opened as a best security practice. Where some systems require a wide range of inbound ports to be open, these can be permitted if bound to very specific IP addresses assigned by the vendor at the source point.

III. SIP/ALG – SIP/TLS

A. For consistency across districts, SIP/ALG will be enabled on firewalls in all instances and will not be disabled.
B. It is preferred to limit ports to only the SIP service and let SIP-ALG open and close ports as needed. We can open port ranges as an alternative, but will not disable SIP-ALG.
C. Solutions must incorporate either SIP/TLS or internal or proprietary End to End Encryption (E2EE).
D. Existing operational SIP/ALG (non-SIP/TLS or E2EE) configurations will be “grandfathered” in, however, all future requests for SIP connectivity will be required to follow all KETS security policies and technical requirements listed above regarding SIP/ALG, SIP/TLS and E2EE.

IV. Introduction of Additional SIP Trunks

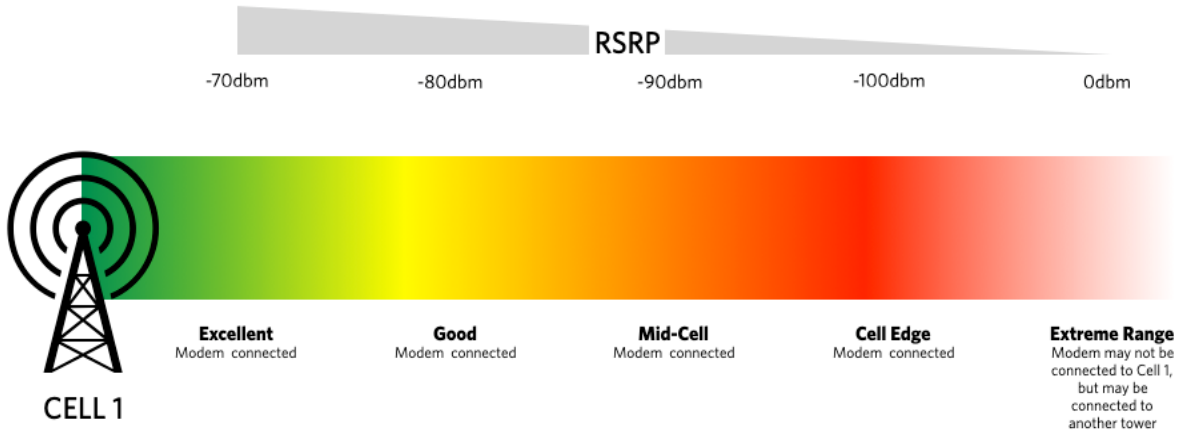
A. SIP trunks are no longer isolated inbound voice communication lines but are technically an alternate Internet connection.
B. New or additional SIP trunks using a non-KEN circuit will not be permitted.
C. Existing operational SIP trunk configurations will be “grandfathered” in if their usage is dedicated to voice services and left unchanged.

V. Cellular Connectivity

A. If the vendor solution is dependent on Cellular connectivity, a Site Survey with confirmation of consistent cellular signal at all service points, including all impacted buildings, is required to prove reliability and connectivity.
1. CDF/MDF/IDF locations and data centers will need to be verified for consistent cellular signal.

B. Because of the significance of emergency services that could be dependent on the solution, a recommended signal strength (RSRP) between -60 dbm and -90 dbm should be observed with a signal quality level (RSRQ) between -5 dB and -15 dB for the best ensured results of service and performance.
C. The chart below illustrates the signal and quality levels for cellular service.

RF Quality	RSRP (dbm)	RSRQ (dB)
Excellent	>= -80	>= -10
Good	-80 to -90	-10 to -15
'Mid Cell'	-90 to -100	-15 to -20
'Cell Edge'	< -100	< -20



The cellular service should be used for the designated purpose and primary use for telecommunication for POTS line replacement for emergency communication services. Vendor administration access will be restricted to the KDE VPN service for primary connectivity, with secondary/out of band connectivity permitted via LTE/Cellular.

VI. Primary Vendor Administration Access/KDE VPN

A. Vendors will remotely access any of the district located physical systems via the KDE VPN secured network connectivity.

1. Vendors will receive an account from the Office Education Technology (OET) and access to the specific systems through this secured connectivity.
2. Vendor's accounts will be managed by KDE/OET security policies.
3. If vendors require multiple support personnel to access systems, separate accounts are required. KDE does not permit the sharing of accounts.
4. Vendors may also use screen sharing services directly with districts (i.e. Microsoft Teams or Cisco Webex).

VII. Additional Recommendations

A. It is not recommended to have multiple PBX servers (i.e. 1 per building).

1. It is recommended to have no more than one PBX servicing the district with a possible failover system if the district requires high resilience.
2. When multiple PBX hardware is introduced in a single district's phone system, various issues with DID calling and extension calling between the PBX systems develop, within both the district's network environment and the KETS Services environment.

B. E911 Services need to be factored into any proposed Voice solution & systems. These to include:

1. Kari's Law
2. RAY BAUM's Act

Glossary

dB: (Decibel, abbreviated as dB, and also as db and DB) In electronics and communications, the decibel is a logarithmic expression of the ratio between two signal power, voltage, or current levels.
dbm: (decibel-milliwatts or dBmW) is a unit of level used to indicate that a power level is expressed in decibels (dB) with reference to one milliwatt (mW).
E911 Services: Enhanced 911 (E-911 or E911) is a system used in North America to automatically provide the caller's location to 911 dispatchers.
Firewall: A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.
Inbound/Outbound Network Traffic: Inbound traffic originates from outside of the district network and is traveling “IN” towards the district network. Outbound traffic originates inside the district network and is traveling “OUT” to an Internet destination.
Ingress/Egress Network Traffic: Ingress refers to traffic that enters the boundary of a network. This may also be referred to as inbound traffic. Egress refers to any traffic that exits an entity, or a network boundary. This may also be referred to as outbound traffic.
KEN: Kentucky Education Network, usually associated with the KEN Rack or KEN Shared Services. The KEN Rack is a network rack located in each KY K-12 School District and houses the KEN Shared Services. The KEN Shared Services include Internet services, managed router, managed firewall and other services provided to the school district.
KETS: Kentucky Education Technology System, refers to various systems and services used to provide Internet connectivity, security and operational services provided by the Kentucky Department of Education of the behalf of Kentucky K-12 School Districts.
Router: is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.
RSRP: A modem determines which tower to connect to on the basis of a value called **RSRP** (Reference Signal Received Power). This is the measured power of the LTE reference signals spread across the broadband and narrowband portions of the spectrum. RSRP values, presented in dBm, are always negative, and the higher the number, i.e. the closer to zero it is, the higher the power of the signal.
RSRQ: The LTE specification defines a second value, **RSRQ** (Reference Signal Received Quality), as the ratio of the carrier power to the interference power: essentially this is a signal-noise ratio measured using a

standard signal. A connection with a high RSRQ should be good, even if the RSRP is low: the modem is able to extract the information in the weak signal because of minimal noise.

SIP/ALG (Session Initiation Protocol Application-Level Gateway): defined as a function within many routers. It inspects any VoIP traffic to prevent problems caused by firewalls and if necessary modifies the VoIP packets. Routers will often have SIP ALG activated by default.

SIP/TLS (Transport Layer Security): SIP/TLS encrypts the data contents within the communication connection between endpoints. Using SIP over TLS allows you to bypass ALG (Application Layer Gateways) and ISP Blocking and still provides a secured connection.

End-to-end encryption (E2EE): is a method of secure communication that prevents third parties from accessing data while it's transferred from one end system or device to another. In E2EE, the data is encrypted on the sender's system or device, and only the intended recipient can decrypt it.

TCP/IP Ports (General): A number assigned to user sessions and server applications in an IP network. Port numbers, which are standardized by the Internet Assigned Numbers Authority (IANA), reside in the header area of the packet being transmitted and thus identify the purpose of the packet (Web, email, voice call, video call, etc.).

TCP/IP Ports (Server Applications/Destination Ports): Destination ports may be "well-known ports" (0-1023) for the major Internet applications, such as Web and email. For example, all port 80 packets (HTTP packets) are directed to and processed by a Web server. User "registered ports" (1024-49151) are assigned to applications that are mostly vendor specific, such as Zoom.

TCP/IP Ports (User Sessions/Source Ports): The source port is a next-available number assigned by TCP/IP to the user's machine. This assigned client number is how the network address translation (NAT), which typically resides in the router, determines which user to send back the responses to.

VoIP (Voice Over Internet Protocol): is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.

VoIP Cloud Based Service: is hosted at your VoIP provider's data center, rather than at your location. Also known as a cloud phone system or off-site VoIP.

VPN: a Virtual Private Network (VPN) is a mechanism for creating a secure connection between a computing device and a computer network, or between two networks, using an insecure communication medium such as the Public Internet.

Additional References and Documentation

KETS_Voice_Guidelines.docx

KETS Network Services Standard