Pexip Service
Security and Privacy Whitepaper

Version 5.6
2024.03.07

Table of Contents

Introduction **5**

Culture of Security and Compliance **5**

What does this mean for you as a customer? 5

Pexip Service High-Level Overview **6**

Pexip Service Data Centres 6

Personal Identifiable Information (PII) **7**

Corporate Customer Relationship Management (CRM) PII 7

Pexip Service PII 8

Pexip Service Registration Data 8

Pexip Service Call Data Records (CDRs) 8

Conference Media 9

Pexip Service Data Processing 9

Use of Sub-Processors 10

Pexip Service Data Storage and Logs 10

Storage Location 11

Key Management 11

Provisioning, Registration and Call Flows **12**

Provisioned and Registered Endpoints 12

My Meeting Video Clients 13

Internal Transcoding and Registered Device Call Sessions 14

Third-Party Unregistered Endpoints 15

SIP Endpoints 15

H.323 Endpoints 15

Point-to-Point Sessions 15

On-Net P2P Sessions 16

Off-Net P2P Sessions 16

Virtual Meeting Rooms (VMR) 16

Live Streaming and Recording 17

CVI for Microsoft Teams 17
Microsoft ExpressRoute for CVI 18
PII sent to Microsoft for CVI calls 19
PII received from Microsoft for CVI calls 19
Google Meet Interoperability 20
PII sent to Google for Google Meet Video Interop calls 21
PII received from Google for Google Meet Video Interop calls 21
Interoperability with other Third-Party Platforms 22
One-Touch Join for Pexip Service 22
OTJ Role-Based Access Control 24
OTJ Meetings API 25
OTJ Endpoint Authentication 25
OTJ Encryption 25
OTJ Data Storage and PII 25
Bring Your Own Carrier (BYOC) 26
PII with BYOC 27
Web Portals 27
Pexip Control Center (PCC) 27
PCC Access 27
PCC Role-Based Access Control 27
PCC Authentication 28
PCC Data Storage and PII 28
Pexip Web App 28
Web App Access 28
Web App Role-Based Access Control 28
Web App Authentication 29
Web App Data Storage and PII 29
Pexip Partner Portal and Analytics 29
Portal and Analytics Access 29
Portal and Analytics Role-Based Access Control 29
Portal and Analytics Authentication 30
Portal and Analytics Data Storage and PII 30
Proactive Security Auditing and Monitoring 30

Software Composition Analysis (SCA) 31
Common Vulnerabilities and Exposures Tracking 31
Vulnerability Scanning 31
Penetration Testing 31
Threat Modelling 31
Security Events 31
Appendix A – Glossary of Terms 33
Appendix B – Data Protection Laws 36

Introduction

Pexip delivers a video conferencing Software-as-a-Service (SaaS) that is hosted in a managed cloud network for small to large business, enterprise, and public sector customers. This service enables customers across a wide range of industries to communicate and achieve their core missions via a global network.

This document is intended to introduce customers and potential customers to the implementation of the security frameworks and compliance processes fundamental to programs such as ISO 27001 in a real-world global cloud service delivery model.

Culture of Security and Compliance

Pexip uses secure system design principles, industry-standard encryption, and strict access control protocols to minimise the risk of unauthorised participants accessing confidential user and organisational data. The Pexip Service has been developed from the ground up using a Defence-in-Depth cybersecurity architecture to provide multiple layers of cybersecurity to our customers and their data. Our comprehensive cybersecurity architecture methodology is designed to address all aspects of the threat model, including *application*, *network*, and *operational* security elements.

Pexip has implemented a Secure Software Development Life Cycle (SSDLC), which enables us to constantly roll out new features, new capabilities, and provide ongoing maintenance and fixes. Our security practises align with internationally recognised compliance standards such as ISO and focus on the organisation holistically. This approach encompasses such diverse business functions as: facility access security procedures; our hiring policies and employee security policies; our SSDLC; and our service monitoring and sustainment practices.

What does this mean for you as a customer?

We have formalised internal information security best practices and implemented the ISO/IEC 27001 standard. Pexip's Information Security Management System (ISMS) is certified, developed, and maintained according to the ISO/IEC 27001 standard with additional security controls from ISO/IEC 27017 for cloud service providers, and additional privacy controls for protection of personal data from ISO/IEC 27018. Pexip has also implemented a Privacy Information Management System (PIMS) which serves as a framework for managing personal data as a data processor (PII processor). The Pexip PIMS is certified, developed, and maintained according to the ISO/IEC 27701 standard. These certification programs are independently audited by DNV, an independent expert in assurance and risk management, headquartered in Norway.

We have formalised a management review of the ISMS and its performance, as well as dedicated Information Security (InfoSec) and Security Operations (SecOps) teams that are responsible across the company and service network. Our company meets the requirements of relevant regulatory,

contractual, and other legal obligations across locations and regions where Pexip operates its cloud services.

Pexip upholds high standards of information security, privacy and transparency for its customers, partners, and employees. We ensure customer data is private, protected, secure, and compliant with all relevant privacy regulations such as General Data Protection Regulation (GDPR)/EU Regulation 2016/679. See **Appendix B – Data Protection Laws** for other examples.

Our video collaboration service is continuously tested with technology providers including Microsoft, Google, Cisco, and Poly to ensure high-quality video conferencing between platforms.

We are committed to proactive testing of both our software solutions and our SaaS offering, the Pexip Service, to ensure they comply with international security standards. We conduct both Static and Dynamic Application Security Testing (SAST/DAST), as well as active penetration testing with a certified third-party auditor.

Pexip Service High-Level Overview

This Security Whitepaper focuses on the Pexip Service SaaS offering, including its architecture, workflows, components, and operations. The Pexip Service solution provides a rich set of features and solution components for customers to consume. Pexip Service may be licensed “a la carte”, choosing only specific features for a solution, or may be licensed with an all-inclusive Pexip Connect Standard licensing bundle.

The following diagram depicts at high-level the available Pexip Service features:

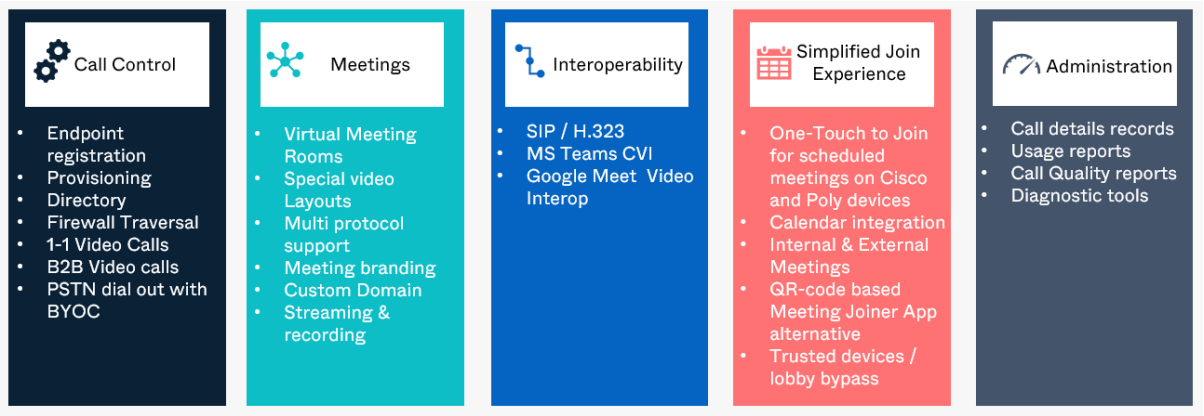


Fig. 1. Pexip Service Features

Pexip Service Data Centres

Multiple geographically dispersed data centres throughout the world combine to form the Pexip Service global network. Pexip contracts with multiple Infrastructure-as-a-Service (IaaS) providers to

deliver a secure environment that provides interoperability, flexibility, scalability and high availability for real-time video and audio communications. Intelligent routing ensures that the Service directs calls and registrations to the nearest Point-of-Presence (PoP) location.

The data centres supporting the Pexip Service are carrier neutral Tier 2 and 3 providers with global presence. Data centre provider facilities are compliant with System and Organisation Controls Type 2 (SOC 2) evaluation criteria in accordance with Statements on Standards for Attestation Engagements 18 and 22 (SSAE18 / SSAE 22). Each data centre provider is ISO 27001 and ISO 9001 certified.

In accordance with Pexip's ongoing organisational ISO 27001 certification program, Pexip enforces physical and remote access controls to ensure only a limited subset of staff are authorised to access Pexip Service production and administrative systems.

Fig. 2. Pexip Service PoPs with Google PoPs and Microsoft PoPs

Personal Identifiable Information (PII)

Personal Identifiable Information (PII), also known as Personal Data in some territories, is any information that can identify an individual. Pexip does not process personal information beyond what is required for the functioning of the Pexip Service. Pexip follows privacy laws listed in

Appendix B – Data Protection Laws.

Corporate Customer Relationship Management (CRM) PII

CRM PII is defined within Pexip as personal data that may be collected, processed, or transferred as part of the normal business of Pexip Service customer relationship activities, such as Sales, Customer Success, or Support efforts and communications. This data is not necessarily included in the Pexip Service itself but is adjacent to the Service in function. CRM PII includes:

- Full name
- Email address
- Telephone number
- Title/Job Function

Pexip Service PII

Pexip Service PII is personal data that may be collected, processed, or transferred related to provisioning and use of the Pexip Service SaaS offering. This includes registration data, Call Data Record (CDR), log data, and conference media data.

Pexip Service Registration Data

The Pexip Service captures PII during customer registration. This is associated to an Enterprise User License and may be enabled for logging into Pexip Control Center (PCC).

The following PII has a retention period of up to six months following the duration of the service contract:

- Display name
- Email address
- Video address
- If assigned personal video endpoint
    - Video address
    - Display name

Pexip Service Call Data Records (CDRs)

Use of the Pexip Service will automatically generate Call Detail Records (CDRs). CDRs allow subscribers and their organisations to track call activity to confirm appropriate use and to permit accurate billing. Access to CDRs and video device registration data is accessible to authorised Pexip staff and reseller partners for the purpose of supporting end-user subscribers.

The Pexip Service retains CDR PII for a period of three months with some exceptions regarding service logs as described below.

CDRs include the following data:

- Meeting title[1]
- Meeting participant names
- Call log details
    - Display names / usernames of participants
    - URIs and / or IP addresses of participants
    - Telephone numbers
    - Call duration
    - Service Logs

Certain CDR fields, such as *Meeting Title*, may or may not contain PII depending on participant and organisational choices.

The Pexip Service retains audit and operations to support service monitoring and management. Pexip retains standard logs for a period of three months. Logs linked to security incidents may be retained for up to three years.

The following PII may be included in Pexip Service logs:

- PII in CDRs
- Email address
- Display name
- IP addresses
- Location

Conference Media

The Pexip Service may process or transmit the following media data during any videoconference session. Conference media data is not persistent in the Pexip Service and has a retention period of zero days.

- Audio streams
- Video streams
- Content sharing
- Profile pictures
- Chat messages

Pexip Service Data Processing

Pexip acts as either the Data Processor or Data Sub-Processor for the personal data an end-user provides to us when activating and / or use of the Pexip Service through any of the Pexip partners who are authorised to sell the Pexip Service or products or software. A user of the Pexip Service is the Data Subject, and the end Customer organisation is the Data Controller. When Pexip acts as the Data Sub-

[1] Only applicable to Pexip Service VMRs

Processor, all processing of personal data (PII) by Pexip will be governed by a Data Processing Agreement (DPA) between Pexip and the Partner. This DPA will constitute Pexip's legal basis for the processing. Direct DPA can also be setup between a customer and Pexip. In this case Pexip acts as the Data Processor.

Pexip's DPA for the Pexip Service clearly explains and defines our commitments regarding GDPR obligations like: Pexip acting as the Data Processor or Sub-Processor; Compliance with laws; Processing of personal data (PII); Transfer of personal data abroad; Use of Sub-Processors and Security measures.

Use of Sub-Processors

Pexip AS, all its subsidiaries and all its parent companies (collectively "Pexip") uses Sub-Processors to provide the best experience and service to Partners, end Customers, and end Users when using the Pexip Service.

A Sub-Processor is a third-party Data Processor engaged by Pexip, who has or potentially will have access to or process Service data or personal data (PII). Pexip engages different types of Sub-Processors to perform various processing functions.

Pexip undertakes to use reasonable selection process by which it evaluates through conducting a Data Protection Impact Assessment (DPIA) or Data Transfer Impact Assessment (DTIA) of the security, privacy, and confidentiality practices of Sub-Processors that will or may have access to or process Service data and personal data (PII). Pexip requires its Sub-Processors to satisfy equivalent data protection obligations as those instructions documented from Data Controllers on Pexip, in such a manner that the processing will meet the requirements of applicable Privacy Laws (refer to

Appendix B – Data Protection Laws)

The current list of Pexip's Sub-Processors and their associated processing activities and locations can be found on the Pexip Service Help website: https://help.pexip.com/service/subprocessors.htm

Pexip Service Data Storage and Logs

The following diagram shows Pexip's data-at-rest (DAR) storage architecture. The Pexip Service maintains three Point of Presence (PoP) host types: Google Cloud Platform (GCP), Microsoft Azure, and Pexip-owned.

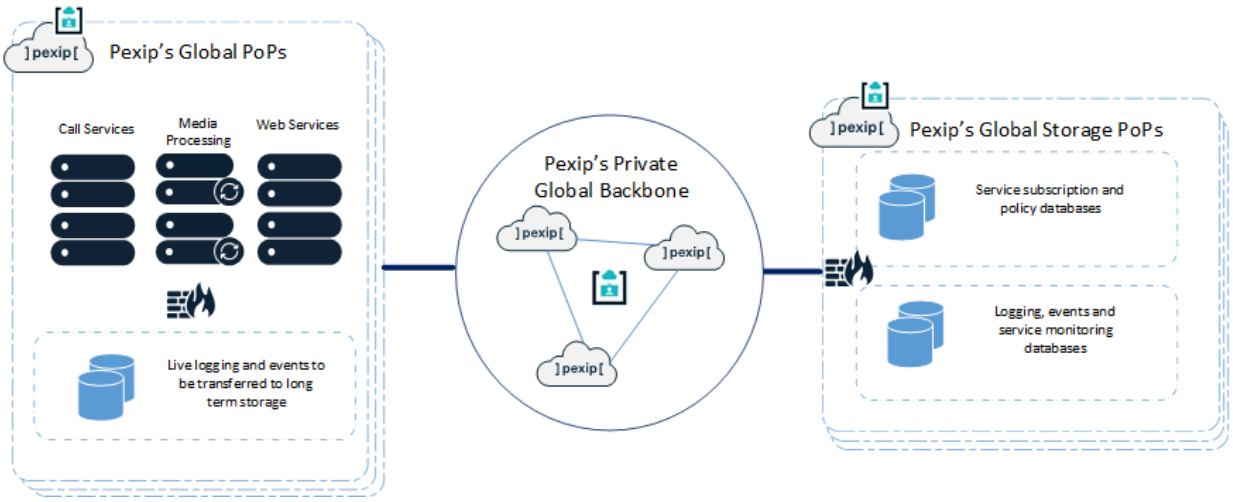


Fig. 3. Pexip Service data-at-rest (DAR) storage architecture

Pexip stores all PII at rest using the Advanced Encryption Standard (AES). Specifically, the Pexip Service uses AES-256 to ensure that an attacker cannot access system or subscriber data without access to the private encryption keys. Pexip applies encryption independently of the Point of Presence (PoP) type.

Pexip backup systems ensure that data remains encrypted throughout the backup process. Pexip Service backup systems are independently encrypted with their own keys.

Storage Location

Pexip stores call- and registration-related PII in the European Economic Area (EEA). The Pexip Service stores limited data sets temporarily in service application databases across the Pexip network of PoPs. Pexip uses this data to orchestrate and report on conferencing services.

Pexip stores CRM PII and Enterprise User License / Registration PII in the United States and the EEA.

Key Management

The Pexip Service generates and stores cryptographic keys in a secure manner that prevents loss, theft, tampering or compromise. Pexip maintains strict access control with the principle of least privilege to read, write and modify the cryptographic keys.

Pexip employs Google Key Management for GCP deployments and Azure Key Vault for MS Azure deployments.

Provisioning, Registration and Call Flows

The Pexip Service offers calling capabilities for standards-based video devices. Pexip has defined a series of distinct call flows for Pexip-registered, third-party platform registered (e.g., Cisco, Poly, Avaya), and unregistered standards-based devices.

In this section we will address the call legs between the customer's device (for Pexip registered endpoints and unregistered devices) or the customer's edge device (for third-party platforms) and the Pexip Service edge.

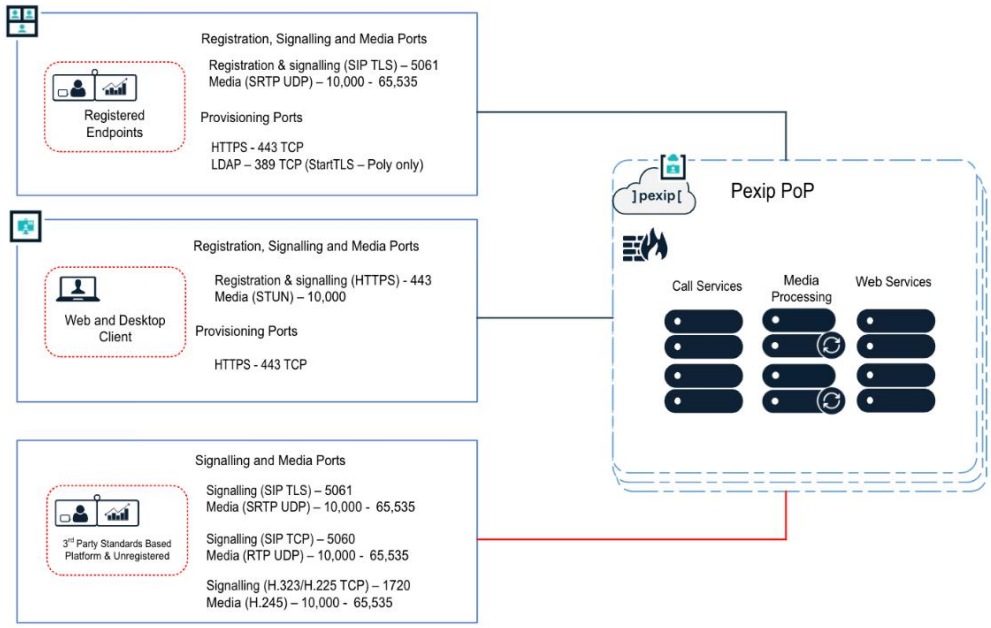


Fig. 4. Pexip Service Provisioning, Registration and Call Ports and Protocols

Provisioned and Registered Endpoints

Provisioned devices provide the most reliable way to enforce a secure call between the endpoint and the Pexip Service, as the Service specifies the protocols that will be used by the device. By design,

registering endpoints to the Pexip Service provides an initial layer of security, as the organisational network perimeter is not exposed to third parties. All calls for registered devices are routed through the Pexip global network.

Customers can further limit their exposure to the public Internet by restricting the organisational IP address spaces reserved for video conferencing to those owned and managed by Pexip. This approach allows the endpoint to place outgoing calls and receive incoming calls via the Pexip global network. In this workflow, the endpoint acts as the traversal client and a Pexip registrar acts as the traversal server.
Customers preferring to have a closer connection may negotiate peering with Pexip's transit providers via local IX (Internet Exchange).

During the provisioning process, the endpoint can either be provisioned by the Pexip *Activate Endpoint* application or automatically provisioned using inbuilt provisioning functions implemented by the device manufacturer. As indicated in **Fig. 4. Pexip Service Provisioning, Registration and Call Ports and Protocols**, the endpoint establishes secure connections to the provisioning servers using TLS-encrypted web services and downloads an XML document with the subscription provisioning data.

This document includes:

- Pexip SIP registrar Fully Qualified Domain Name (FQDN)
- System name
- Uniform Resource Identifier (URI)
- Authentication Credentials
- Phonebook
- Network Time Protocol (NTP) Server
- Preferred call settings

After receiving the provisioning information, the endpoint will register to the Pexip call registrar using the SIP protocol.

!	**Endpoints default to SIP TLS over port 5061 using TLS 1.2 or later but securing the endpoints remote access policy is the device administrator's responsibility**

Pexip provides Enhanced Room Management (ERM) software that enables endpoint resource and configuration management to assist with endpoint management and local device security configuration.

My Meeting Video Clients

The video software client native to the Pexip Service is a self-authored application named My Meeting Video (MMV). MMV is available for the Microsoft Windows and Apple macOS, as well as Android Smartphone/Tablet, and iPhone/iPad (iOS) mobile device platforms.

Subscribers of the Pexip Service can sign in using their e-mail address or video address, and their password, to register to the Pexip Service to initiate or receive video calls. Users may utilise SAML 2.0 based Single Sign-On (SSO) operated by their preferred Identity Access Management provider to sign into their accounts.

The Pexip Service provisioning server provides the MMV client with registration information upon the user logging in to the application. MMV clients register to the nearest service registrar. The Pexip API manages provisioning and registrar communication via a secure TLS v1.2-encrypted Hypertext Transfer Protocol Secure (HTTPS) and WebSocket Secure (WSS) tunnel.

The MMV Client uses HTTPS encrypted signalling that facilitates ease of deployment. The client encrypts media using the IETF Datagram Transport Layer Security Extension for the Secure Real-time Transport Protocol (DTLS-SRTP). To maximise connectivity the client deploys Session Traversal Utilities for NAT (STUN) and Traversal Using Relays around NAT (TURN) with an additional TCP port 443 failover. Please see the *Web and Desktop Client* illustration in **Fig. 4. Pexip Service Provisioning, Registration and Call Ports and Protocols** for further information.

All MMV calls to VMRs or between MMV clients are transcoded. Calls route through a service gateway to connect to SIP or H.323 services.

Internal Transcoding and Registered Device Call Sessions

Pexip maintains a security posture internally that all calls will be secured wherever possible. Transcoding resources within the network utilise a virtual backplane between locations that are secured for both signalling and media via IPsec tunnels across the Pexip global network. **Fig. 5. Pexip Service Internal Media Sessions** depicts this workflow ‘Inter PoP Call Security’. Transcoded signalling and media traffic from the SIP proxies, registrars and RTP relays use SIP TLS and SRTP if a registered endpoint or external SIP endpoint uses TLS.

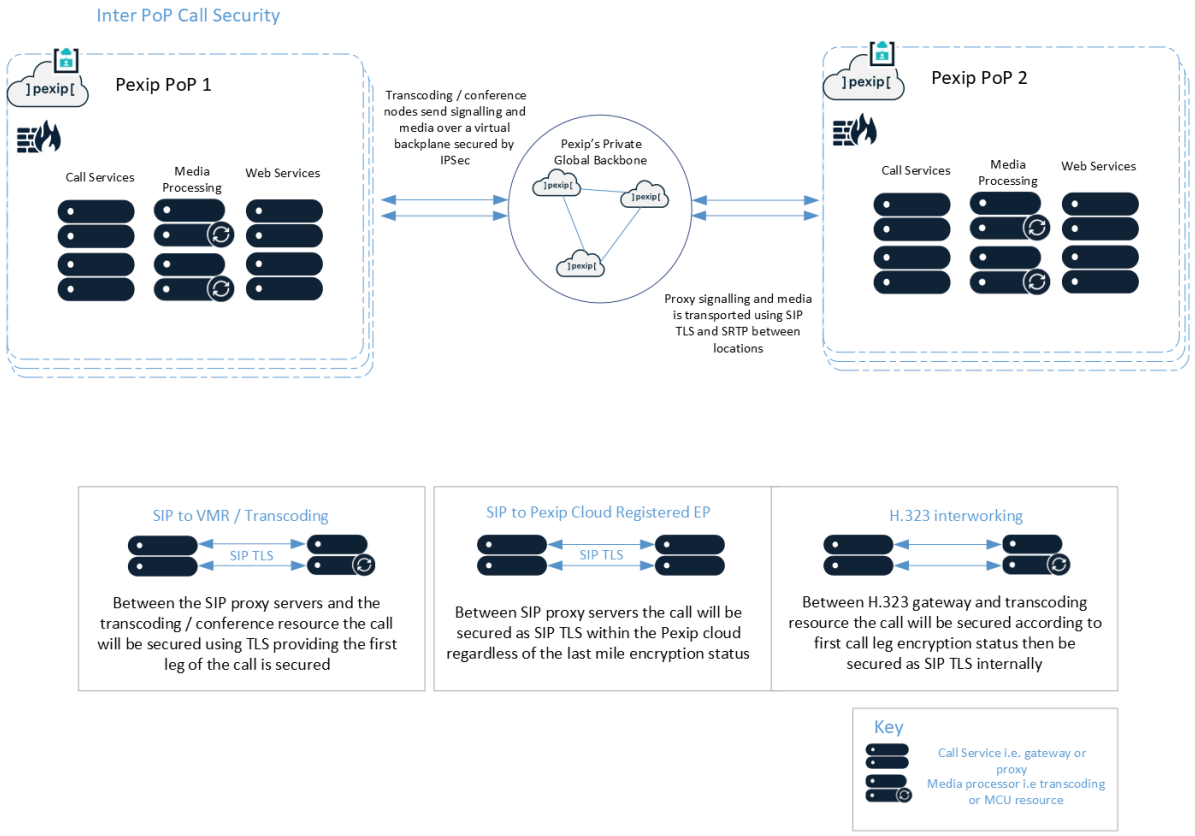


Fig. 5. Pexip Service Internal Media Sessions

Third-Party Unregistered Endpoints

Pexip uses a best effort encryption posture with third-party endpoints not directly registered to the Pexip Service to ensure the greatest level of interoperability.

> ! **With video conference systems that are *not* registered to Pexip, the onus is placed upon the customer video platform administrator or caller to ensure that their environment is correctly configured to support encryption on the call legs between the customer and Pexip network edges.**

SIP Endpoints

The preferred SIP security posture in all situations is to encrypt the call with SIP TLS, however Pexip supports placing outbound calls or receiving calls using the SIP TCP protocol. SIP TCP does not encrypt signalling messages or media across the application transport layer during video calls.

> ! **Customers should be aware that using insecure protocols such as SIP TCP will put their data at risk.**

For Pexip users calling to or receiving calls from third-party systems, Pexip supports failover to SIP TCP over the last mile path. In the case of the far end party not supporting SIP TLS, the call leg between the Pexip proxy and the far-end will be unencrypted.

H.323 Endpoints

Pexip supports AES media encryption in H.323 in compliance with the ITU-T H.235.1 standard. If media encryption is not enabled in the endpoint, the Service defaults to unencrypted calls to maintain interoperability.

> ! **To ensure data privacy, Pexip strongly recommends that users and organisations conduct calls using SIP TLS whenever possible.**

Point-to-Point Sessions

The Pexip Service supports Point-to-Point (P2P) calls within the network of subscribers directly registered to the Pexip Service, as well as calls between a subscriber and an external party.

On-Net P2P Sessions

For P2P calls within the network of subscribers directly registered to and provisioned by the Pexip Service Network, Pexip encrypts all internal call-legs. The Pexip Service requires that video devices registered to and provisioned by the Service Network must support SIP-TLS v1.2 or above for signalling and a minimum of 128-bit encryption SRTP for media. Under this scheme, signalling and media between each stage (hop by hop) in the end-to-end call flow may only use encrypted protocols as shown in **Fig. 5. Pexip Service Internal Media Sessions**.

Off-Net P2P Sessions

For P2P calls with an external party, the Pexip Service performs interworking with external SIP and H.323 video devices. SIP-only calls connect via the SIP Proxy Server to which the subscriber is registered. SIP-to-H.323 calls connect via the registered SIP Proxy Server and route through an interworking gateway which performs SIP to H.323 transcoding. The interworking gateway supports H.235 secure media encryption for H.323 and SRTP for SIP as shown in **Fig. 5. Pexip Service Internal Media Sessions**

The Pexip Service supports P2P calls where the external party either fully or partially supports encryption. If the external party cannot support encryption, the call will be allowed to connect, but the call-leg between this external party to the closest stage in the end-to-end call flow will be unencrypted.

Virtual Meeting Rooms (VMR)

VMRs provide the capability for multiple participants to meet in a multiparty call to collaborate, as well as serve as the gateway for interoperability between disparate video-enabled and audio-only communities including standards-based H.323, SIP, and WebRTC participants and Public Switched Telephone Network (PSTN) dial-in parties.

VMRs are configured to negotiate encryption with participants if the party can support this capability. Each party connected to a VMR port is connected as a P2P call between itself and the MCU resource handling the call for the VMR as shown in **Fig. 6. Pexip Service Virtual Meeting Room Call Flow**

The Pexip Service supports VMR calls where the external party either fully or partially supports encryption. If the external party cannot support encryption, the call will be allowed to connect, but the call-leg between this external party to the closest stage in the end-to-end call flow will be unencrypted.

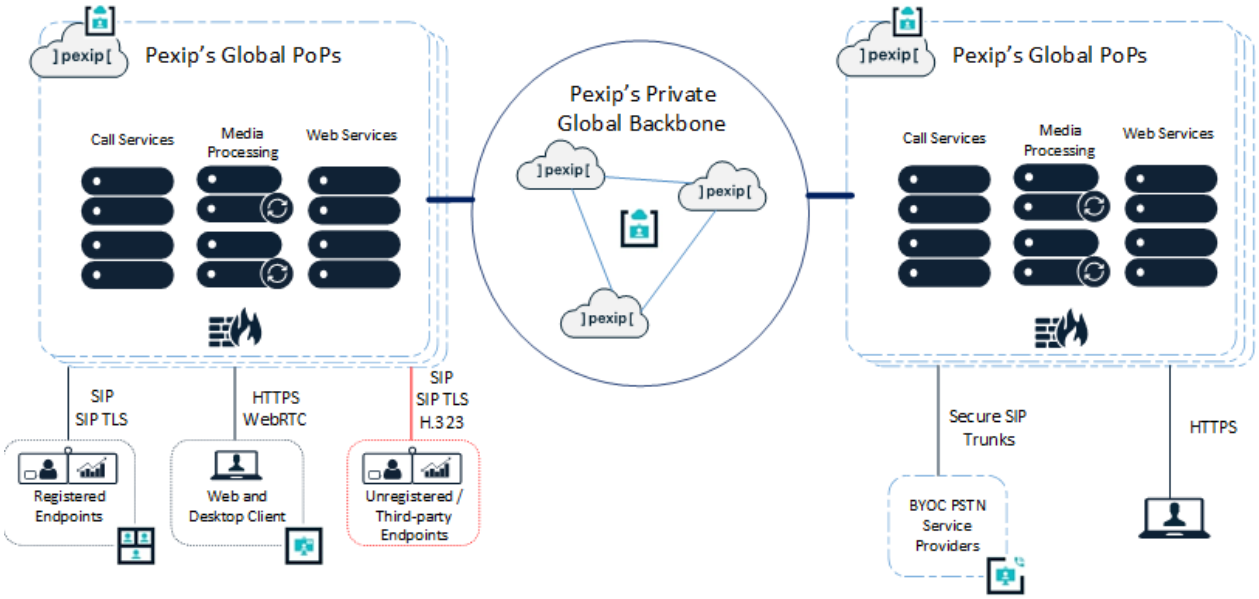


Fig. 6. Pexip Service Virtual Meeting Room Call Flow

Live Streaming and Recording

The Pexip VMR Service provides the capability for subscribers to configure integration with external third-party streaming and recording services. Using this feature a VMR meeting administrator can efficiently deliver meeting content to a mass audience, as well as record and distribute it for archival purposes.

The Pexip Streaming and Recording feature uses the Infinity MCU platform supporting the Pexip VMR Service to transmit to compatible third-party streaming ingestion services using Real-Time Messaging Protocol (RTMP) or Secure RTMP (RTMPS) traffic. Please note that such third-party services lie

outside the Pexip service boundary. Pexip Streaming and Recording has no impact upon third-party authentication or privacy policies.

CVI for Microsoft Teams

Pexip is a Microsoft Certified Cloud Video Interop (CVI) service provider. CVI is a Microsoft-provided interoperability solution between Microsoft Teams and standards-based endpoints, such as SIP and H.323 video systems. Microsoft requires that all service providers deploy CVI resources exclusively on the Azure Platform-as-a-Service (PaaS) offering.

The Pexip Service deploys a dedicated application, known as Pexip Teams Connector, to perform CVI interworking between the native Pexip Service environment and the customer's Microsoft Teams environment. Each Teams Connector is a secured and hardened Windows virtual machine (VM) instance which is deployed within Azure as part of a Virtual Machine Scale Set (VMSS).

Pexip utilises SIP-TLS and HTTPS as the signalling protocols and SRTP as the media protocol for application layer traffic between Service gateways, transcoding locations, and Pexip Teams Connector. Media processing occurs internally to the Pexip Service environment prior to being transmitted to the Teams Connector gateway environment in Azure.

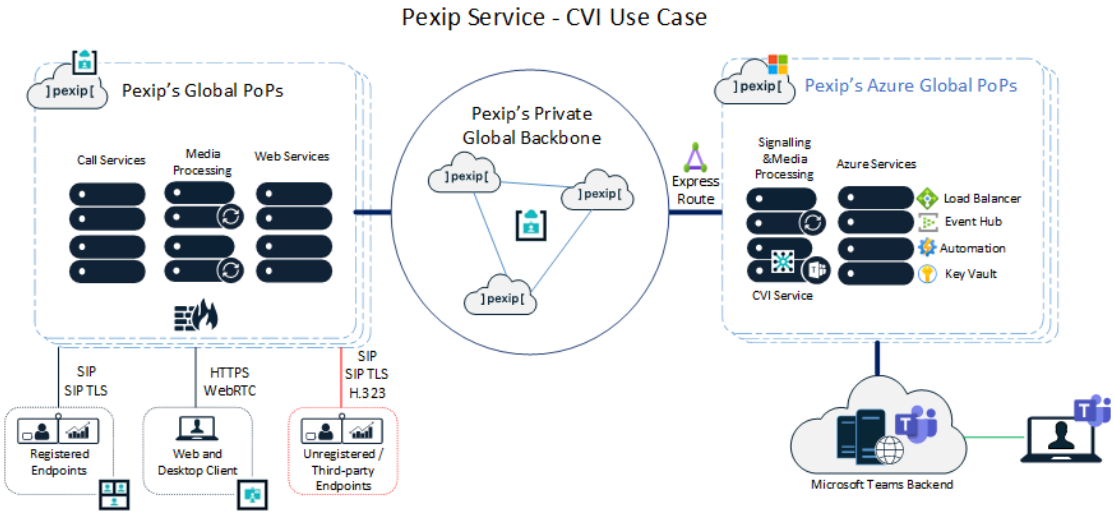


Fig. 7. Pexip Service CVI Call Flows

Pexip's standard Microsoft Teams interoperability solution allows video conferencing endpoints to join Microsoft Teams meetings that you are hosting. Onboarding to this service requires consent to be granted to the Pexip Teams application by a Teams tenant administrator.

"SIP Guest Join" (SGJ) is a feature that allows video conferencing endpoints to join Microsoft Teams meetings, where that meeting is being hosted by an external third-party organisation who has not enabled Pexip interoperability. The feature set of this service is restricted in comparison to Pexip's standard Microsoft Teams interoperability solution since no application consent needs to be granted.

Microsoft ExpressRoute for CVI

Microsoft ExpressRoute is a dedicated private circuit that secures the physical transport layer of the signalling and media flow between the nearest Pexip PoP and Microsoft Azure. Pexip currently provides interconnects from the Pexip network over Microsoft ExpressRoute connections for this service in the following locations:

- West Europe (Netherlands)
- East US 2 (Virginia)
- West US (California)
- Australia East (New South Wales)
- Southeast Asia (Singapore)
- Japan East (Tokyo)

Fig. 8. Pexip Service PoPs in Microsoft Azure for Teams CVI

PII sent to Microsoft for CVI calls

The Pexip Service transmits the following endpoint data to Microsoft Teams for CVI calls:

- Display Name
- SIP Uniform Resource Identifier (URI)

Customer organisations that choose to use PII in endpoint naming schema will thus be exposing PII to Microsoft Teams. Pexip has no control over customer endpoint naming conventions.

CVI meeting data is subject to Microsoft's data retention policy. As customers must authorise the Pexip Service to connect to the organisational Teams instance, customers consuming CVI have already accepted Microsoft's terms and conditions for data storage.

PII received from Microsoft for CVI calls

The Pexip Service receives the following Microsoft Teams client user data (roster information) for Microsoft Teams for CVI calls:

- Display Name
- User Object ID (universally unique ID in Azure Active Directory, assigned to a user)
- User Principal Name (user@domain)[2]
- Azure Active Directory profile picture[2]

On the video feed displayed on standards-based video endpoints in the CVI meeting, the Display Name is shown in real time, along with the Azure Active Directory profile picture if the user is connected audio only.

Pexip Control Center meeting troubleshooting will also show the Display Name and User Principal Name in real time.

Pexip does store in its Service logs and CDRs the Display Name and User Principal Name – this is stored encrypted at rest in accordance with Pexip's Service Data Retention Standard.

Google Meet Interoperability

For those customers using the Pexip Service as a gateway for Google Meet interoperability, Pexip operates transcoding resources in Google Cloud Platform (GCP). Customers already partnering with Google may access Pexip SIP registrars, SIP proxies, and H.323 gateways via data centre peering, providing high quality carriage to these PoPs.

Pexip currently provides interconnects from the Pexip network over the Google Meet gateway in the following locations:

- Netherlands — europe-west4
- Frankfurt — europe-west3
- Singapore — asia-southeast1
- Sydney — australia-southeast1
- Oregon — us-west1
- N. Virginia — us-east4

[2] Not applicable to SIP Guest Join

Fig. 9. Pexip Service PoPs in GCP for Google Meet Interop

The Pexip Service routes inbound signalling and media through the Pexip network to the GCP Global PoPs as shown in **Fig. 10. Pexip Service Google Meet Interop Call Flows**.

Pexip Service transcoding resources in the GCP Global PoPs interwork standardised signalling protocols to the Google Meet protocol. Signalling and media are encrypted using HTTPS and SRTP between Pexip and the Google Meet platform.

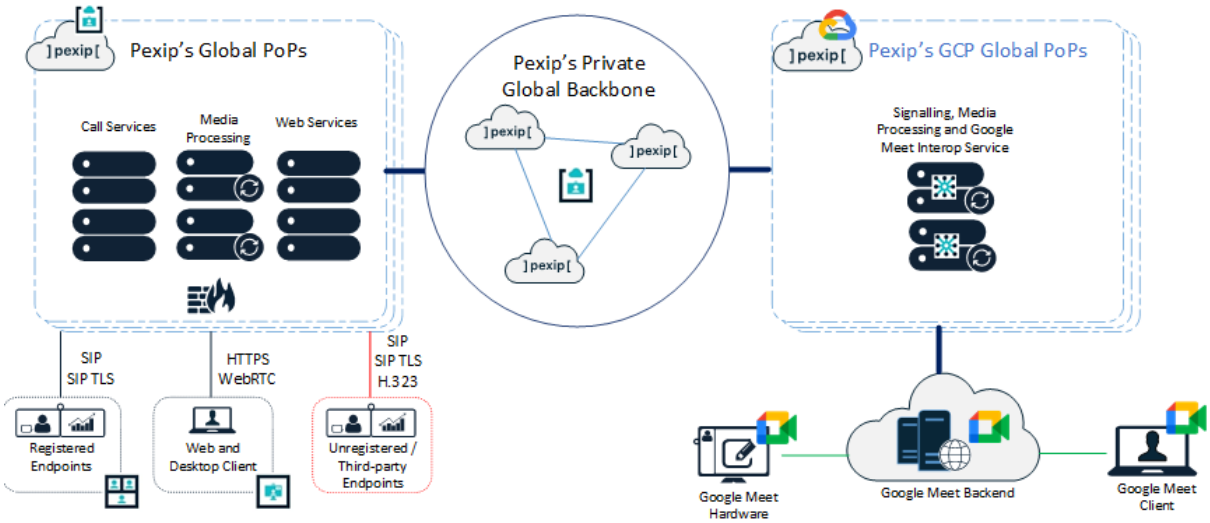


Fig. 10. Pexip Service Google Meet Interop Call Flows

PII sent to Google for Google Meet Video Interop calls

The Pexip Service transmits the following endpoint data to Google for Google Meet calls:

- Display Name
- Endpoint User Agent (UA)

Customer organisations that choose to use PII in endpoint naming schema will thus be exposing PII to Google. Pexip has no control over customer endpoint naming conventions.

The endpoint UA, although not classed as PII, includes the make, model and software version of the videoconferencing device used.

Google Meet call data is subject to Google's data retention policy. Customers consuming Google Meet have already accepted Google's terms and conditions for data storage.

PII received from Google for Google Meet Video Interop calls

The Pexip Service receives the following Google Meet client user data for Google Meet Video Interop calls:

- Display Name

On the video feed displayed on standards-based video endpoints in the Google Meet Video Interop meeting, the Display Name is shown in real time.

Pexip Control Center meeting troubleshooting will also show the Display Name in real time.

Pexip does store in its Service logs and CDRs the Display Name – this is stored encrypted at rest in accordance with Pexip's Service Data Retention Standard.

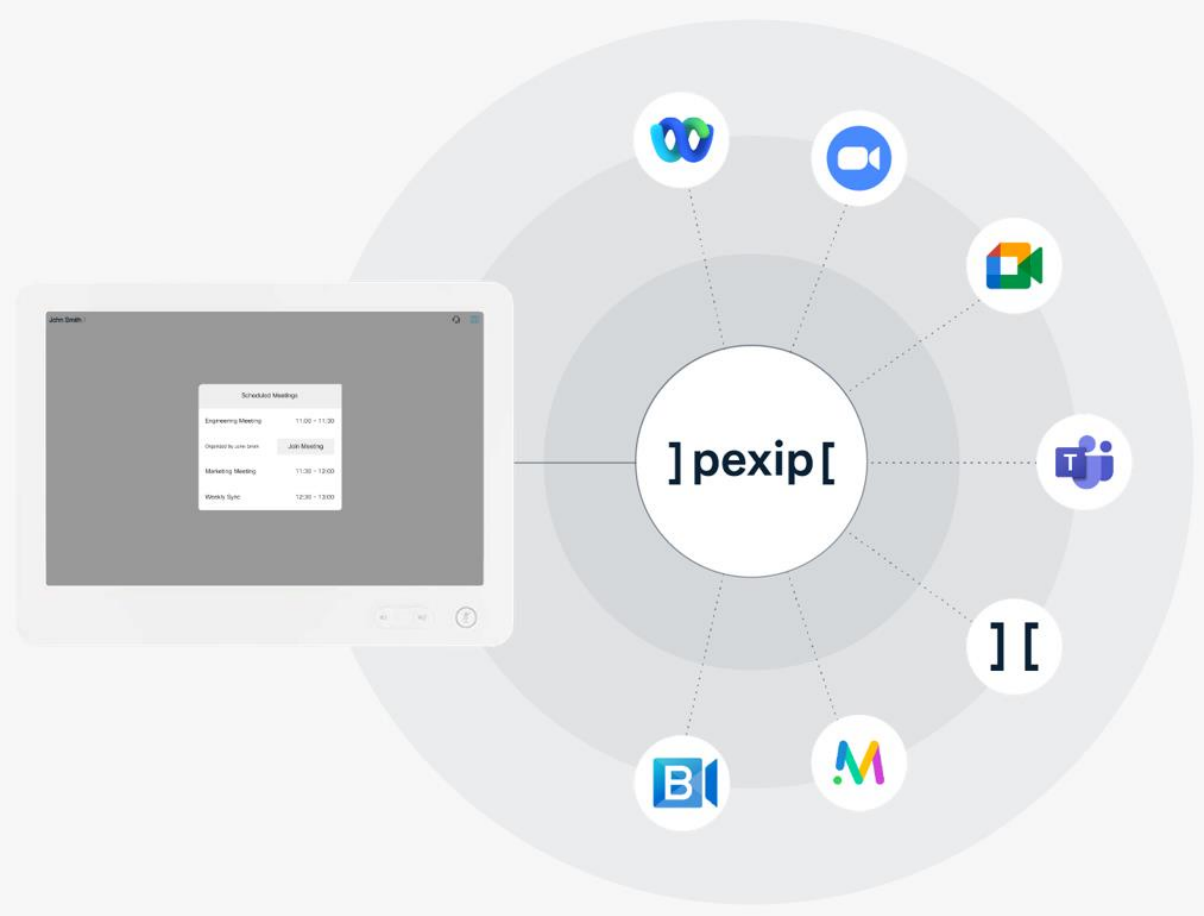
Interoperability with other Third-Party Platforms

Pexip customers may interface between Pexip and third-party video platforms, such as Zoom or Webex, using standards-based SIP. In these scenarios, Pexip can only validate the security of the session within the Pexip boundary. Customers leveraging third-party services should evaluate the data security and privacy standards of those platforms to minimise the risk to their organisational data.

One-Touch Join for Pexip Service

One-Touch Join for Pexip Service (OTJ) integrates support for "click to join" videoconferencing endpoint workflows for numerous popular video meeting services into a customer's Pexip Service tenant. This is supported for a range of Cisco and Poly videoconference endpoints (https://help.pexip.com/service/otj-about.htm#endpoints) for integration with Microsoft 365 tenants and

mailboxes only. The Cisco endpoints once enabled will display a **Scheduled Meetings** button on the home screen which lists all the meetings scheduled on that device for the day. Shortly before a meeting begins a **Join** button appears within the **Scheduled Meetings** list and in a separate notification that appears on the touch panel, allowing the user to simply press a single button to join their meeting. For Poly endpoints once enabled, the meetings will show in the native Poly calendar specific to the endpoint type.



Cisco endpoints configured for use with One-Touch Join for Pexip Service require a macro written by Pexip known as the OTJ macro to be installed on the endpoint. The installation of such macros is a standard feature provided by Cisco for their modern endpoints.

Poly endpoints configured for use with One-Touch Join for Pexip service use the native Poly calendar experience.

One-Touch Join for Pexip Service is either enabled or disabled for an entire customer tenant and is configurable through **Pexip Control Center (PCC)**.

The following diagram shows the high-level architecture of One-Touch Join for Pexip Service:

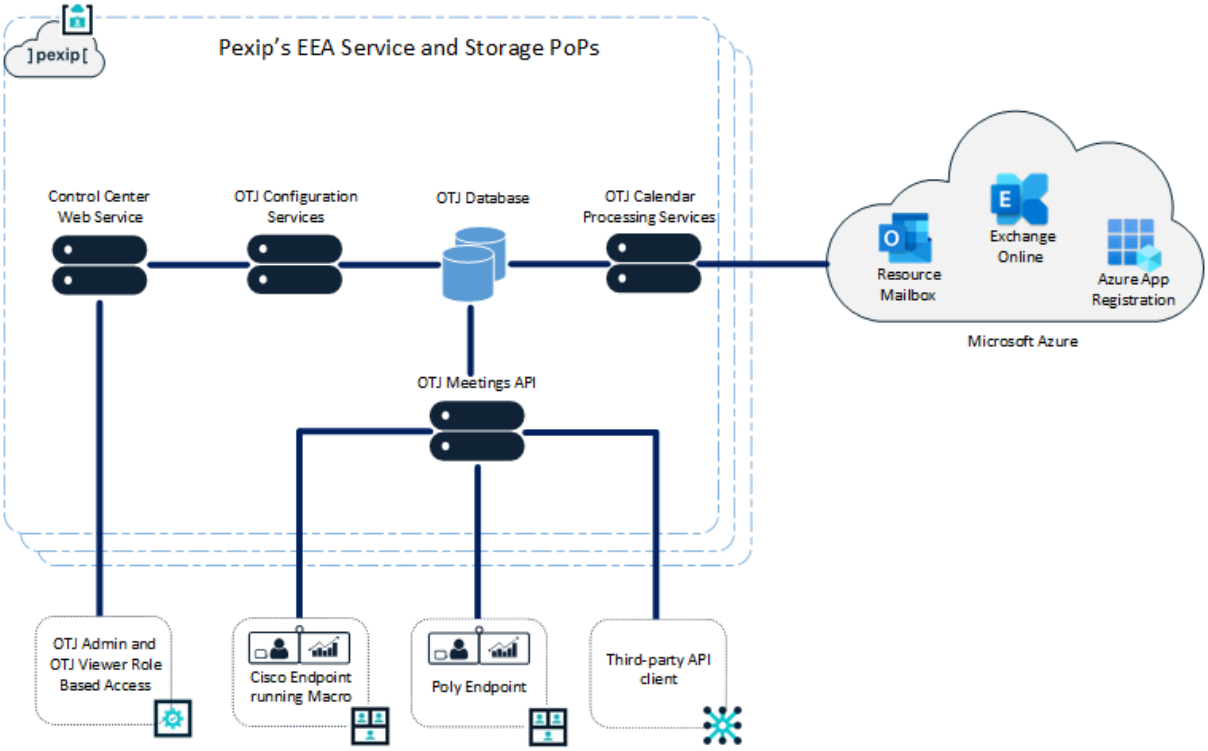


Fig. 11 - One-Touch Join for Pexip Service Architecture

OTJ Role-Based Access Control

Pexip OTJ and SRE Development teams have Identity Access Management (IAM) permission in GCP, where One-Touch Join for Pexip Service is hosted, to read the contents of the OTJ database. These permissions are managed and controlled by a group that is strictly locked down to only the members of these teams, following the principles of Role Based Access Control and Least Privilege control framework. These people can read the contents of the database however they cannot read any of the confidential data outlined under **OTJ Data Storage and PII** because this is encrypted before being added to the database.
Outside of Pexip's OTJ and SRE Development teams, administrator-level access for viewing and editing the configuration of OTJ for the organisation is handled through **Pexip Control Center (PCC)**.

In addition to the roles outlined under **PCC Role-Based Access Control** the following roles may be granted to members of an organisation, provided they already have the Admin role associated to their user account in PCC.

- **OTJ Viewer** – this role gives the user already with Admin role the additional ability to view but not edit the OTJ settings for the organisation and to view but not edit the macro for OTJ settings for individual Cisco videoconference systems in the same organisation.

- **OTJ Admin –** this role gives the user already with Admin role the additional ability to view and edit the OTJ settings for the organisation and to enable OTJ for individual videoconference systems, including editing and downloading the OTJ macro for Cisco videoconference systems or obtaining the Poly OTJ credentials.

OTJ Meetings API

One-Touch Join for Pexip Service provides an externally accessible API which can be used to get a list of the next meetings for a video system. The API connection is unique for each video system within each organisation and cannot be used to access calendar information from any other video systems either in the same organisation or in other organisations. Furthermore, the API does not provide access to any other elements of the Pexip Service.

When a Cisco video endpoint is configured for One-Touch Join for Pexip Service in Pexip Control Center, a client ID and client secret is generated as part of the configuration, and this is required to authenticate to the API. When a Poly video endpoint is configured, the OTJ username and password is generated by Pexip Control Center and this is required to authenticate to the API. Strict rate limiting is imposed on the API with a recommendation of one request per minute per client with a maximum of 10 requests per minute permitted.

OTJ Endpoint Authentication

One-Touch Join for Pexip Service API uses the OAuth 2.0 client credentials grant flow to obtain an access token that can be used to access the Meetings API. To get the access token, a HTTPS POST request needs to be made and the client ID and client secret generated in Pexip Control Center must be sent in the Authorisation header using the Basic authentication scheme. The response includes an access token that is used in the Meetings API request and is valid for a one-hour period.

OTJ Encryption

All meeting data in transit between video endpoints and the OTJ Meetings API and in transit between the Pexip OTJ Calendar Processing API and Microsoft Exchange Online is encrypted using HTTPS. Within the Pexip OTJ environment, data in transit is sent using Cloud Pub/Sub which individually encrypts incoming messages as soon as the message is received and uses Google-managed encryption keys.

All confidential data as defined in **OTJ Data Storage and PII** is client-side encrypted using Google KMS before being inserted into the data store. Encryption keys are rotated every 30 days. The confidential data alongside all other data is further encrypted at rest in the data store using Google’s default encryption.

OTJ Data Storage and PII

One-Touch Join for Pexip Service stores the following data which contains or might contain PII:

- Meeting subject
- Meeting organiser name
- Meeting organiser email address
- Meeting start time
- Meeting end time
- SIP alias
- Mailbox address

Confidential data such as meeting subject, meeting organiser name, meeting organiser email address and SIP alias is encrypted using Google's default encryption before being inserted into the database.

Data is stored at rest in GCP in the EEA.

Pexip strongly recommends setting up a mail-enabled security group in Microsoft Exchange Admin Center which only contains the mailboxes for use by videoconference systems with OTJ, otherwise Pexip would have access to read all calendars in the customer organisation. With the security group enabled, Pexip only has access to read the calendars of those video conference systems enabled for OTJ.

Bring Your Own Carrier (BYOC)

Bring Your Own Carrier (BYOC) allows video endpoints registered to the Pexip Service on SIP to dial out to PSTN destinations such as landline phones, mobile phones and conferencing services supporting audio dial-in. This avoids the need for separate audioconference phones in meeting rooms. Pexip Service customers using the BYOC option establish a SIP trunk / carrier peer connection to the telephony carrier of their choice.

Pexip delivers the outbound call from the videoconference system to the chosen carrier, which then handles the rest of the call. Depending on the carrier capability it can also be possible to map incoming telephony calls to specific Pexip Service registered video endpoints as a secondary feature. This uses a dedicated direct inward dial number per video endpoint.

For outbound calling the user places a call from their Pexip-registered video endpoint using a prefix that tells Pexip Service which telephony carrier and which number / caller ID is to be used for the call. Pexip will first route the call to the closest currently available Pexip Service PoP. Pexip will then route the call via its global network to the carrier.

The carrier may at this point request authentication details in the form of a SIP username and password. Whilst this is optional Pexip highly recommends that customers deploy this configuration

for security purposes. Customers should also enforce SIP TLS for signalling encryption. For the final step, the carrier accepts the call and delivers it to the destination PSTN.

Customers may also deploy a session border controller (SBC) for the BYOC service. Pexip configures and tests SBCs on a case-by-case basis and the details around the security of these devices will not be addressed in this whitepaper.

PII with BYOC

Caller IDs from mobile phones or landlines dialling into the Pexip Service via the BYOC service will be logged in the Pexip Service Call Detail Records (CDRs) and logs and are accessible via Pexip's analytics portals. Data retention policy for this data will be in line with other CDRs and log information for the Pexip Service, defined in Pexip's Service Data Retention Standard.

Web Portals

All Web Portals delivered by Pexip communication on the wire use HTTPS. Any connections on HTTP are redirected to HTTPS services.

Pexip Control Center (PCC)

Pexip Control Center (PCC) is a web-based portal available to Pexip customers, Pexip partners and Pexip employees, which brings the admin and analytics tasks for all users (company administrators and end users) into one place.

PCC Access

At a high level, access to an organisation's information in Pexip Control Center is based on a parent-child hierarchy model. Administrators and users within an end customer organisation only have access to their own data. Administrators in a Pexip partner organisation have access to their own organisation's data as well as those of its own customers. Administrators within Pexip have access to Pexip's own organisation data, as well as those of its partners and their customers.

PCC Role-Based Access Control

Within Pexip Control Center role-based access control is enabled. There are three primary roles which can be granted to members of an organisation, each consuming a Pexip Service End User License (EUL):

- **User** – anyone with a Pexip Service EUL effectively can login to Pexip Control Center using the same account credentials and will have access to their own personal data only. This role is not specifically granted, rather is inherited by default.
- **Admin** – a user with the Admin role granted can view all the data for their entire organisation.
- **Access Admin** – this role must be granted in addition to the Admin role and gives the administrator additional capability of being able to manage user roles within Control Center

and therefore promote users to have the Admin role or Admin role with Access Admin role.

Pexip employees and Pexip Partners with the Access Admin role can grant users access in other organisations provided they themselves have the rights to view the data in those organisations and only in accordance with the parent-child hierarchy model.

PCC Authentication

Sign in to Pexip Control Center leverages the same credentials as a Pexip Service End User account as per section **Web App Role-Based Access Control**. Authentication is either via a username and password stored in the Pexip Service or alternatively organisations may enable SAML 2.0 based Single Sign-On operated by their preferred Identity Access Management provider.

To protect the user data, Pexip has ensured that no user passwords that are managed and stored by Pexip are stored in plain text. Please note that the only way to restore a user password is to utilise the approved password recovery tool.

PCC Data Storage and PII

Pexip Control Center itself does not store data or PII. The data is that stored already in Pexip Service and Control Center simply provides a pane of glass to view the data at rest.

Pexip Web App

The Web App provides company users with a web browser-based video client as well as company administrators with a portal for managing their user, shared VMRs and endpoint subscriptions.

Web App Access

Administrators and users within any organisation only have access to their own organisation's data through this portal – namely the users, shared VMRs and endpoints in the same organisation.

Web App Role-Based Access Control

Roles are granted by the Pexip Partner Portal which is only accessible to Partners and Pexip employees. There are effectively 2 roles which can be granted to members of an organisation, each consuming a Pexip Service End User License (EUL):

- **User** – anyone with a Pexip Service EUL effectively can login to their account for access to call and VMR using the same account credentials and will have access to their own personal data only. This role is not specifically granted, rather is inherited by default.
- **Admin** – a user with the Admin role granted can view all the data for their entire organisation. This user is able assign PINs to VMRs and control conferences. Admins also can add and remove users from a company.

Web App Authentication

Sign-in to Web App requires a Pexip Service End User account. Authentication is either via a username and password stored in the Pexip Service or alternatively organisations may enable SAML 2.0 based Single Sign-On operated by their preferred Identity Access Management provider.

To protect the user data, Pexip has ensured that no user passwords that are managed and stored by Pexip are stored in plain text. Please note that the only way to restore a user password is to utilise the approved password recovery tool.

Web App Data Storage and PII

Pexip WebApp is both a video client and management tool. Data that is stored by Pexip may include first name, last name, username and password, application PIN & preferences, RTMP service information, account CDR and service logs relating to call history. Data retention policy for this data will be in line with other CDRs and log information for the Pexip Service, defined in Pexip's Service Data Retention Standard.

Pexip Partner Portal and Analytics

The Pexip Partner Portal is a partner focused CRM tool designed to handle account management of customers utilising the Pexip Service. This provides the ability to assign licensing, configure services and create user/device subscriptions.

Analytics is a partner tool providing detailed metrics and call data on customers using the Pexip Service. Functionality of this tool is being transitioned in to the Pexip Control Center which will replace this tool.

Portal and Analytics Access

At a high level, access to an organisation's information in Partner Portal is based on a parent-child hierarchy model. Administrators and users within a partner organisation only have access to their customers data. Administrators in a Pexip partner organisation have access to their own organisation's data as well as those of its own customers. Administrators within Pexip have access to Pexip's own organisation data, as well as those of its partners and their customers.

Portal and Analytics Role-Based Access Control

Roles are granted by the Pexip Partner Portal which is only accessible to Partners and Pexip employees. Access to Analytics is managed via the Pexip Partner Portal.
There are 3 default roles in the Partner Portal that you can assign to an account:

- **Read-only User** – this level of access only provides the ability to view customer details. No management of accounts is allowed.
- **Regular User** – a regular user has standard rights to manage customer accounts including managing users, VMRs, endpoint subscriptions and domain hosting.

- **Partner Manager** - a partner manager inherits the same rights as a Regular User with the added ability to manage Partner Portal users and change users' roles.

To facilitate granular access to tools and functions secondary roles are implemented.

Secondary Roles

- **Purchaser** – this role allows a user to add paid subscription licenses to the Partner Portal.
- **Analytics Access** – this provides access to the Analytics tool for the Partner Portal user.
- **Analytics Administrator** – this role providers the ability to manage the access to the Analytics tool.

Roles such as Purchaser and Analytics Administrator can only be assigned by Pexip employees.

Portal and Analytics Authentication

Sign in to Pexip the Partner Portal and Analytics uses dedicated user accounts only assigned for this tool. Authentication is via a username and password stored in the Pexip Service. Multi factor authentication (MFA) is required for access to the Analytics tool.

Portal and Analytics Data Storage and PII

To establish the environment necessary for users to consume the Pexip Service, users will need to provide the minimum information so that they can establish unique identities on the Service for call processing and personal account maintenance. At the individual level, user information includes a name and an e-mail address. At the organisational level, information includes endpoints, Microsoft 365 / Google Meet tenant information, contact information for key stakeholders responsible for interaction with Pexip for service announcement, technical, and billing purposes.

Pexip Analytics itself does not store data or PII. The data is that stored already in Pexip Service simply provides a pane of glass to view the data at rest.

Proactive Security Auditing and Monitoring

As part of Pexip's continuing efforts to maintain and improve security of its SaaS offerings we conduct both Static and Dynamic Application Security Testing (SAST/DAST). Wherever possible Pexip Infosec and SecOps teams undertake regular security audits via third-party and internal assessors. These audits include policy reviews, compliance audits, personnel interviews, vulnerability, and penetration testing utilising various threat models on live production systems.

These audits are used to identify limitations and vulnerabilities of mission critical services and assist in providing remediation paths for procedural, physical, network and application-level system implementation.

Further to this and as part of ongoing auditing and secure software development procedures the following areas are addressed:

Software Composition Analysis (SCA)

Pexip employs continuous processes for scanning third-party libraries and containers for any vulnerabilities. Utilising a developer-first SCA solution, we aim to find, prioritise, and fix security vulnerabilities and license issues in dependencies and transitive dependencies. Pexip's SCA solution makes use of an industry-leading security intelligence database that is maintained by a dedicated research team and combines public sources, contributions from the developer community, proprietary research, and machine learning to continuously adapt to the changing and expanding nature of security threats. This is to ensure that known vulnerabilities are mitigated according to our secure systems development policies.

Common Vulnerabilities and Exposures Tracking

Pexip actively monitors published Common Vulnerabilities and Exposures (CVE) relevant for our products. The vulnerabilities are tracked and mitigated.

Vulnerability Scanning

Pexip deploys state of the art vulnerability scanning tools that are seamlessly embedded into engineering workflows. Currently the Pexip Service is scanned for hundreds of thousands of vulnerabilities from numerous threat sources helping Pexip to quantify risks across our assets.

Penetration Testing

The Pexip Service is penetration tested by an authorised third party at least twice a year. The objective is to determine Pexip's exposure to targeted attacks from an Internet-facing vector. The test is conducted in a manner that replicates malicious actors engaging in targeted attacks utilising various techniques and methods. Customer penetration testing of Pexip Service is not permitted.

Threat Modelling

Pexip includes the process of threat modelling throughout the engineering life cycle from design, through implementation to operation applying industry methodologies such as S.T.R.I.D.E. to identify and mitigate risks.

Security Events

Pexip has follow-the-sun support model for any security events reported by customers, partners or third parties. Pexip processes are in line with ISO 27001:2013 for business and service continuity.

Services and devices within each PoP are closely and continually monitored by an Operations Team 24x7x365. Operations monitoring includes traffic volume, registration activity, subscription management, network path traffic and usage patterns. Notification alarms are dispatched to the team when anomalous activity is detected. The available monitoring information is aggregated and can be accessed through automated tools, which can additionally be used to support security audits.

Appendix A – Glossary of Terms

Term	Description
AES	Advanced Encryption Standard. Standardised by NIST as FIPS-197
AICPA	American Institute of Certified Public Accountants
API	Application Programming Interface
CDR	Call Detail Records
CVE	Common Vulnerabilities and Exposures – a program maintained by the United States' National Cybersecurity FFRDC that provides a reference-method for publicly known information security vulnerabilities and exposures
CVI	Cloud Video Interop – a Microsoft Qualified third-party solution that enables third-party standards-based video conference devices to join Microsoft Teams meetings
DAST	Dynamic Application Security Testing – designed to detect conditions indicative of a security vulnerability in an application in its running state
DPA	Data Processing Agreement – a contractual addendum of written instructions from the data controller (exporter) to the data processor (importer) regarding what PII-data are authorised to be collected, processed, and transferred, including organisational and technical measures to protect the data
DPIA	Data Protection Impact Assessment – a process designed to identify risks arising out of the processing of personal data (PII) and to minimise these risks as far and as early as possible
EEA	European Economic Area
Endpoint	A standards-based video conference appliance used either in a meeting room or in a personal office
FQDN	Fully Qualified Domain Name
H.235	The ITU-T standard for securing H.323
H.323	The ITU-T umbrella standard for video conferencing over IP
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
IAM	Identity and Access Management – permissions that allow organisations control access to the resources in their cloud environments such as Google GCP and Microsoft Azure.
IP	Internet Protocol
ISMS	Information Security Management System – an ISMS provides a systematic approach for managing an organisation's information security, following the guidance of ISO/IEC 27001.

IX	Internet Exchange
MCU	MultiPoint Control Unit – a video / audio bridge to host multiparty conference calls
MMV	My Meeting Video – the name for Pexip's software videoconferencing application for desktop and mobile devices
NIST	The National Institute of Standards and Technology is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce.
NTP	Network Time Protocol
OTJ	One-Touch Join for Pexip Service that integrates a Join meeting workflow to compatible Cisco and Poly video conference systems
P2P	Point to Point
PII	Personal Identifiable Information, also known as Personal Data in some territories, is information that, when used alone or with other relevant data, can identify an individual. Pexip only handles non-sensitive PII
PIMS	Privacy Information Management System – a framework for managing personal data which provides controller and processor specific controls for data privacy, in accordance with the ISO 27701 standard. Pexip has implemented PIMS and is certified to the ISO 27701 standard as a data processor.
PoP	Point-of-Presence – the network interface point between the public Internet or customer network and the Pexip cloud service network. This is located in a physical or virtual data centre which typically also handles call processing
PSTN	Public Switched Telephone Network
RFC	Request For Comments – IETF standards publications
RTMP	Real-Time Messaging Protocol – a network protocol for streaming media over IP networks
RTMPS	RTMP utilising a TLS connection
RTP	Real-Time Transport Protocol – a network protocol for delivering audio and video over IP networks
SaaS	Software as a Service
SAST	Static Application Security Testing – designed to analyse application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities. SAST solutions analyse an application from the "inside out" in a nonrunning state.
SBC	Session Border Controller – a special-purpose device that protects and regulates IP communications flows for real-time communications including VoIP, IP video, text chat and collaboration sessions

SCA	Software Composition Analysis is an automated process that identifies the open-source software in a codebase. This analysis is performed to evaluate security, license compliance, and code quality
SSDLC	Secure Software Development Life Cycle
SIP	Session Initiation Protocol – a communication protocol over IP standardised by the IETF as RFC 2543 and revised in RFC 3261
SIP TLS	SIP utilising a TLS connection.
SOC2	System and Organization Controls Type 2 – Audit reporting standard defined by the AICPA featuring five Trust Service Principles: Security, Availability, Confidentiality, Processing Integrity, and Privacy
SRTP	Secure Real-Time Transport Protocol – a profile for RTP intended to provide encryption to RTP data
SSAE16	Statement on Standards for Attestation Engagements 16 – Auditing standard defined by the AICPA which incorporates the SOC 2 reporting standard
SSAE18	Statement on Standards for Attestation Engagements 18 – Auditing standard defined by the AICPA which incorporates the SOC 2 reporting standard
STRIDE	A model for identifying computer security threats developed by Microsoft. It provides a mnemonic for security threats in six categories – Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege.
STUN	Session Traversal Utilities for NAT – a standardised set of methods, including a network protocol, for traversal of NAT gateways for video, voice and other interactive communications, specified in RFC 5389
TLS	Transport Layer Security, an IETF standard
TURN	Traversal Using Relays around NAT – NAT session traversal protocol specified in RFC 8656
URI	Uniform Resource Identifier
VC	Video Conferencing
VMR	Virtual Meeting Room – Video / audio bridge meeting room that hosts multi-party conference calls
VoIP	Voice over Internet Protocol or IP telephony – a method and group of technologies for the delivery of voice communications and multimedia sessions over IP networks, such as the Internet
WebRTC	Web Real-Time Communication – API definition that supports browser-to-browser applications for voice calling, video chat and point-to-point file sharing without the need of either internal or external plugins

Appendix B – Data Protection Laws

Pexip complies with data protection laws around the world where we process information and protect data subject rights. Examples include:

- EU Regulation 2016/679 (the GDPR)
- EU Regulation 2018/1725
- EU Regulation 2022/2555 (NIS2)
- UK General Data Protection Regulation (UK GDPR)
- UK Data Protection Act 2018 (DPA 2018)
- California Consumer Privacy Act of 2018 (CCPA) as amended by California Privacy Rights Act of 2020 (CPRA) and the California Consumer Privacy Act Regulations as amended or superseded from time to time (the “CCPA”), and any related regulations or guidance provided by the California Attorney General.
- LGPD Brazilian Data Protection Law (LGPD) as amended by Law No. 13,853/2019
- Norwegian Personal Data Act
- Swiss Federal Act on Data Protection (FADP)