Datasheet: Security & Compliance

Overview | Use Cases | Benefits | Commercial Terms | Technical Specifications

tokbox

OpenTok Security

TokBox recognizes that security is an essential consideration for any business interested in integrating real time communications into its website, app or service. The OpenTok platform is a reliable and secure platform on which you can build applications that meet your company, industry or client security needs. We support the latest security capabilities with advanced features to comply with requirements and ensure that sensitive user information remains secure.

HIPAA Compliance + BAA

The OpenTok Platform is HIPAA Compliant and TokBox signs BAA's with companies on the Enterprise package, or on the Growth or Standard package with an additional fee.

Benefits

- The OpenTok platform facilitates secure interaction between end users, such as patients, doctors and care providers.
- Our platform is designed so that you can build HIPAA compliant applications providing that a developer architects their application in a secure way.

Commercial Terms

Included with Enterprise accounts, and is available as an add-on feature for Standard and Growth plans at an additional cost.

Regional Media Zones

Regional Zones gives customers the ability to host media traffic in specific regions, including the US, European Union and Germany, to meet specific compliance requirements of those regions.

Benefits

- Media and signalling traffic are hosted in the desired region
- Complies with stricter data privacy requirements
- TokBox privacy and security policies apply

Commercial Terms

Customers can restrict media to the US, EU or Germany.

- Restricting media to the US and EU is included in the Growth and Enterprise plans, and available as an add on for Standard plans.
- Restricting media to Germany is included in the Enterprise plan, and available as an add on for Growth and Standard plans.

Technical Specifications

- The service deploys the OpenTok media and signaling servers to data centers located in the required region.
- Redundancy is built in so that the loss of a data center in the region will not bring down the whole service
- Clients located outside the region are not blocked from connecting to sessions hosted in the region
- Operational logging data from clients and servers are sent encrypted to a logging server in the US where IP addresses are stripped out. The OpenTok API server may be located outside the region.

Encrypted Archiving

With Encrypted Archiving, archived data is never unencrypted at rest or in transit providing the highest level of security. This enables customers to meet the most stringent of compliance and regulatory requirements.

Benefits

- Data is encrypted both in transit and at rest hence ensuring the highest level of security.
- Useful for Healthcare & Finance customers to meet their strict data privacy compliance requirements.
- Entire workflow can be programmatically managed with easy to use APIs

Commercial Terms

Included in Growth and Enterprise plans, and available as an add on for Standard accounts.

Technical Specifications

- There are two ways to encrypt OpenTok archives:
  1. OpenTok encryption — With OpenTok encryption, video and audio data in an OpenTok archive is encrypted using a public key certificate you provide TokBox.
  2. Amazon S3 server-side encryption — This uses Amazon S3-managed encryption keys
- Decrypted archive file format - MPEG-TS
- Algorithm used for encryption - AES-256
- Generated password is encrypted using RSA encryption with OAEP padding
- *Encrypted Archiving can only be used with composed archives, not individual stream archives.

AES-256

By default, the media streams passing through the OpenTok platform are encrypted using AES 128-bit encryption. For enhanced security, the OpenTok platform also supports the AES-256 level of encryption on media streams.

When a client is connecting to an OpenTok media server or another client, the cipher to use will be negotiated. If the client supports AES-256 then this will be the cipher negotiated for the media traffic. If the client does not support it, then AES-128 will be used. In the case of Relayed sessions, both clients must support AES-256, otherwise they will fall back to AES-128.

Benefits

- Have confidence data is secure with the highest-level of bit encryption
- Useful for customers who work with highly-confidential data and restrictive networks

Commercial Terms

Included with Enterprise plans, and available as an add-on for Standard and Growth accounts.

Technical Specifications

AES-256 is supported (in addition to AES-128) in apps that use the following OpenTok client SDKs:

- OpenTok iOS 2.13+
- OpenTok Android 2.13+
- OpenTok.js 2.13+ running on Chrome 62+

  (with a flag set) or on Firefox 56+. On Chrome 62+, you can enable AES-256 by enabling the Negotiation with GCM cipher suites for SRTP in WebRTC setting in the chrome://flags page.

Only AES-128 is supported in apps that use the following OpenTok client SDKs:

- OpenTok Windows SDK
- OpenTok.js 2.13+ running on Safari or the OpenTok plugin for Internet Explorer
- OpenTok 2.12 or older

IP Whitelisting

TokBox maintains a list of IP address blocks for media and HTTP traffic. These details can be shared with Enterprise customers so that they can limit exposure of their network to trusted endpoints only.

Benefits

- Gives IT departments peace of mind as they can now open up their networks to a select set of IP addresses and not wildcard domain names. In the process it makes the video solutions that our customers are building more enterprise-ready
- Useful for Telehealth and Finance customers who work with restricted networks, and open up their firewalls to trusted endpoints only.

Commercial Terms

Available to Enterprise customers only.

Technical Specifications

- TokBox will provide a 90-day advance notice to customers using the published IP address blocks
- Customers would be expected to use the updated list of IP address blocks published by TokBox. Failure to stay up-to-date with the latest IP address blocks published by TokBox will lead to disruption of service.
- List of IP address blocks associated with the platform components on the enterprise line is made available to enrolled customers. This list includes the following components:
  - Media servers
  - TURN servers
  - API server
  - Logging servers

Contact us

Headquarters:
501 2nd Street
Suite 310
San Francisco, CA
94107

Offices in:
Sydney
New York
Barcelona
London

bizdev@tokbox.com
facebook.com/tokbox
twitter.com/tokbox
linkedin.com/company/tokbox

tokbox

tokbox.com