digitalsamba

# Security White Paper

Last modified: 30 November, 2022

We created Digital Samba to revitalise the traditional video conferencing experience. Our platform is **intuitive, feature-rich, easy to use**, and has **data privacy and security** built into the fibre of its architecture and code base. Companies, organisations and public initiatives worldwide use Digital Samba for their video conferencing and webinar needs and trust our platform to keep their data secure. We strive to keep it that way.

**Data privacy and information security** are integral parts of our company culture. In this whitepaper, you will see how we put our data security philosophy into practice in the various elements of our platform.

We absolutely despise business models where you are the product. And so, we make you this promise: we will **never** sell personal data to 3rd parties. We make our money when you are satisfied with our services and nothing else.

If you have any questions about the security of our platform or want to learn more about our products and how Digital Samba can help you, don't hesitate to contact us.

# Table of Contents

# Secure hosting

What is secure hosting? In its simplest form, secure hosting involves securing access to physical servers in a data centre. But we don't just want basic security- we want all the bells and whistles that only the best data centres can provide. And we only partner with the best.

## SaaS-optimised hosting

The use of SaaS video conferencing services skyrocketed during the pandemic. Countless people and companies flocked to big global players like Zoom, Google and Microsoft to fulfil their demand for remote communication tools. Today, these tools are a part of everyday life, and concerns over their security and privacy are front of mind, particularly their compliance with privacy legislation.

Digital Samba is acutely aware that security and privacy are more important than ever. We have therefore partnered with Leaseweb, a "true" EU-based hosting provider (as opposed to a US-based company with data centres in Europe), to ensure that customer data is secure. As a Tier III provider, Leaseweb caters to large enterprises and provides enterprise-level services, security and uptime. The data centres we work with have direct peering connectivity to the Internet Exchanges, which offers high bandwidth and low latency, a must for high-quality video conferencing.

When it comes to data privacy, Leaseweb data centres hold- and adhere to- the following certifications and compliance standards:

### ISO 27001

ISO 27001 is the international security standard benchmark for the protection of sensitive data. The certification process encompasses organisational security policies, personnel security, physical and environmental security, systems and network security, and business continuity management.

### PCI DSS

PCI DSS confirms the secure handling of sensitive information and helps organisations proactively protect customer data. Leaseweb's certification focuses on physical access safeguards and procedures. Digital Samba only uses PCI DSS-certified Leaseweb data centres.

### SOC 1 (Type II)

A SOC 1 report focuses on outsourced services that could impact a company's financial reporting. In our case, it examines the potential risks faced by Digital Samba regarding its financial reporting as a consequence of using Leaseweb's systems.


### HIPAA

The Health Insurance Portability and Accountability Act defines standards for security controls to protect health information. Leaseweb has obtained a third-party statement from a trusted certification body that recognizes compliance with HIPAA requirements in the Washington DC data centre.


### CISPE

The CISPE Code of Conduct focuses exclusively on the Infrastructure-as-a-Service (IaaS) sector. Auditors accredited by the European Data Protection Authority verify compliance with the code, assuring we can leverage Leaseweb as part of our overall GDPR compliance initiative.

We have worked with numerous data centres since we set up shop in 2003 and learned some tough lessons along the way. Leaseweb has been nothing short of exceptional since we first partnered with them back in 2018. If you are interested in diving a little deeper into everything to do with Leaseweb, have a browse through the resources they provide on their website.

## Denial of Service protection

The data centres we work with provide standard DDoS Protection out of the box. They use globally located detectors and scrubbing centres that recognize and protect against volumetric- and protocol-based DDoS attacks on your servers.

We then add a layer of protection by working with Cloudflare, which provides unmetered mitigation of volumetric DDoS attacks at Layers 3, 4, and 7. Cloudflare can absorb bitrate attacks up to 37 Tbps and packet rate attacks up to 750 million packets per second.

## Systems and software architecture

We only provide details of our technical architecture upon request. Please get in touch to see if we can accommodate you. Note that you must sign an NDA if the request is approved.

## Hosting locations

Leaseweb gives us access to 25 data centres globally, and we have selected a subset to work with. Our choice of data centre is based on two things:

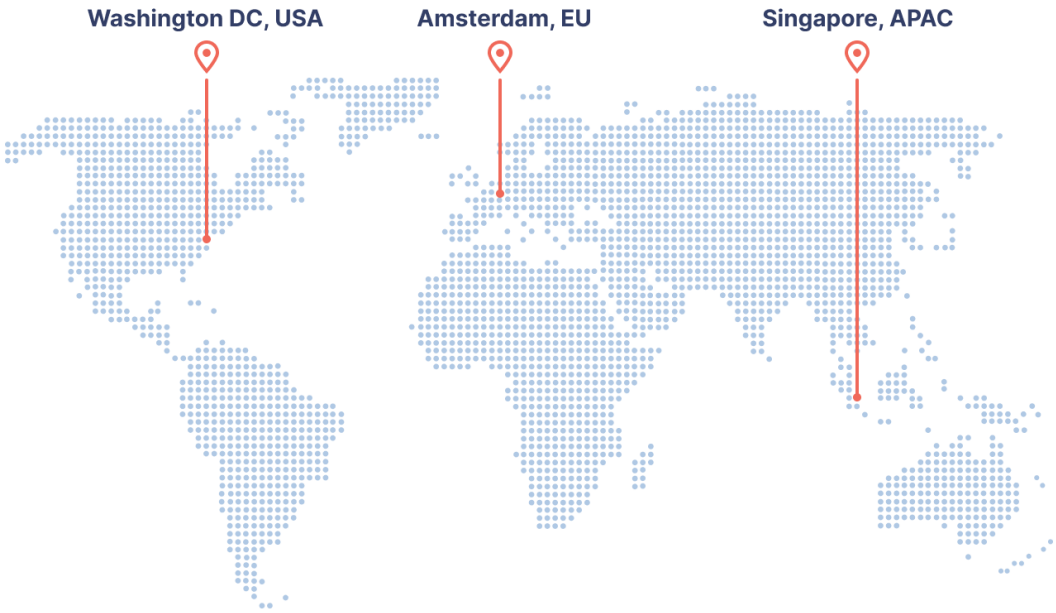
1. Proximity to an Internet Exchange
2. Compliance and certifications

Based on these criteria, we work with the following data centres:

- Amsterdam, Netherlands (AMS-01)

- Frankfurt, Germany (FRA-10)
- Washington D.C., USA (Manassas, VA) (WDC-02)
- Singapore (Serangoon) (SIN-01)

Note that Cloud Server customers can choose their preferred/must-have geographic location when signing up.




## On-premise hosting

Digital Samba software can be deployed as an on-premise option on your hosting infrastructure. This gives you full control over operational, legal and security requirements. Talk to our sales team for more information about on-premise software deployments.

# Cryptography and communications security

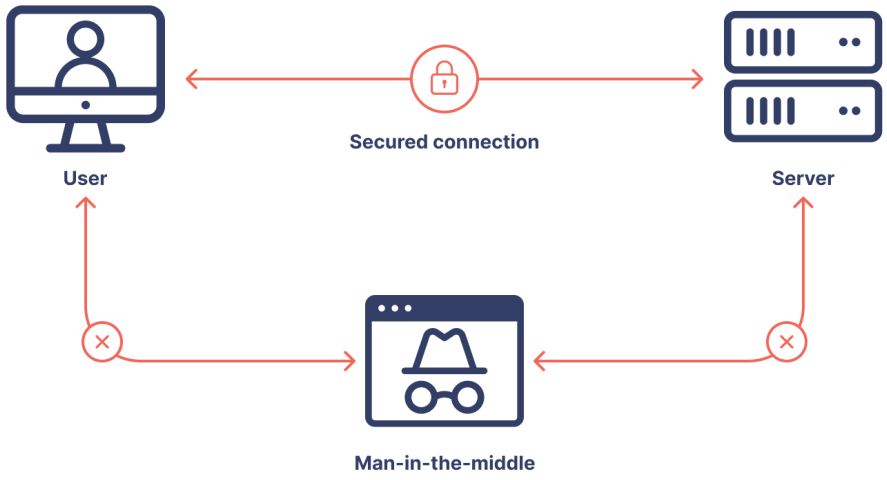
Information is a valuable asset, and access must be managed with care to guarantee that confidentiality, integrity and availability are maintained. Encryption of information helps mitigate the risk of unauthorised disclosure and tampering. It also ensures that access to Digital Samba assets is only granted to those with authorization.

## Transport encryption

TLS (Transport Layer Security) is the industry standard for transport encryption. It ensures that eavesdroppers and hackers are unable to see what you transmit. If you transmit data over Digital Samba systems, you can rest assured that strong hashing algorithms and cypher suites are used.

TLS is most familiar through its use in secure web browsing, and you will surely recognise the padlock icon that appears in your web browser when a secure session is established. However, its application goes beyond the browser and is used in things like e-mail, file transfers, video conferencing, instant messaging, voice-over-IP and DNS.

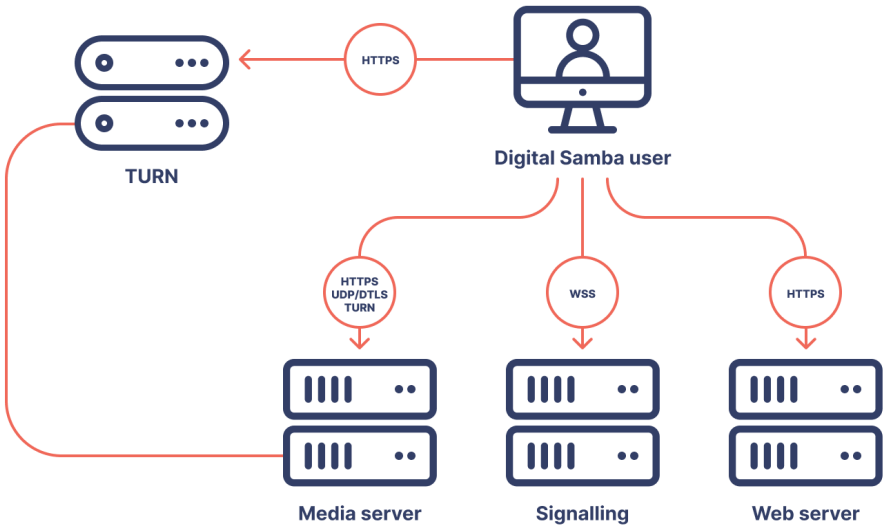
Note that TLS runs on the TCP transport layer. For other transport layers, we use transport encryption that is based on TLS, such as DTLS for UDP.




Transport encryption is implemented across our infrastructure and organisation to prevent perpetrators from being able to execute man-in-the-middle attacks.

## Technical implementation details

Digital Samba products are not limited to client-browser communication. We have more interfaces to protect. Below, you will find detailed information on how we protect all the public-facing interfaces between the user and our infrastructure.




- **User - Web Server.** Data transport occurs on port 443 via HTTPS (TLS encrypted HTTP). Port 80 is exposed purely to facilitate HTTP to HTTPS redirects. All requests on other ports are dropped.
- **User - Signalling Server.** Data transport occurs on port 443 via WWS (TLS encrypted websocket). All requests on other ports are dropped.
- **User - Media Server API.** Data transport occurs on port 443 via HTTPS (TLS encrypted HTTP).
- **User - Media Server.** Video streams are transported on ports in the 1024-65535 range via DTLS-SRTP (UDP). The implementation is based on OpenSSL and libsrtp, which takes care of the DTLS handshake between peer and server and sets up the proper SRTP and SRTCP context.
- **User - TURN Server.** Negotiation is via HTTPS on port 443. If media stream transport is required, it is either over a port in the 1024-65535 range via DTLS-SRTP (UDP), or over 443 via HTTPS (TCP).

Other public-facing components in our infrastructure, including the telephony server and the recording server, are locked down via IP whitelisting, SSH keys and similar mechanisms to prevent unauthorised access.

## Access control

Our access control policy is specified, documented and reviewed regularly. Access to information and applications is restricted following "need-to-know" and "least-privilege" principles. Processes for user registration, de-registration, and access provisioning are in place. We review user access permissions at regular intervals.

## Operations security

Our operating procedures are documented, and changes to information processing facilities are controlled. Development, testing and operational environments are separated to reduce the risk of unauthorised changes to the production environment. Controls to protect against malware are implemented. Information about technical vulnerabilities of information systems are obtained in a timely fashion, and appropriate measures to address the associated risks are taken.

### Data backup

We regularly review and strengthen our security infrastructure and practices, including server backup, data redundancy, and personal data management. Ensuring that data can be restored after corruption or loss is a pivotal part of implementing data protection strategies. Backups of information are taken and tested regularly.

### Event logging

In computing, an event is an action performed by a system, a user, or other external agents. Our systems record all generated events. Most of these events are part of a company's day-to-day, but, in rare cases, they may be a sign of a potential vulnerability or breach. This is where log files come in. These data files are an organisation's first line of defence in the battle against cyber threats. The logs also capture system administrator activity and security events, which are reviewed regularly.

## System acquisition, development and maintenance

When we deploy new systems or enhance existing ones, we carefully scrutinise the security implications of these changes to the system as a whole. The same is true for application development. New and updated systems and applications are thoroughly tested and verified throughout the development process by the development team to ensure that integrity is preserved.

Our applications are developed following industry best practice standards including the Open Web Application Security Project (OWASP) Development Guidelines.

## Incident management

Incident management responsibilities and procedures are in place to ensure quick, effective and orderly response to security incidents. These procedures also cover communication with our service providers and communication with customers and authorities in case of data breaches.


## Product security features

At the product level, we offer several features in our video conferencing software that allow you to protect and moderate meetings and webinars for a secure and disruption-free experience.

- **Lobby.** Place participants in a waiting room before letting them in.
- **Broadcasting permissions.** Individually turn video and audio for participants on/off.
- **Remove participants.** Remove or ban disruptful participants.
- **Specific invite links.** Create user-specific invitation links.
- **Password protection.** Protect your video conference or webinar with a password
- **Roles.** Assign users to a role to limit what they can do.
- **Chat control.** Disable chat, delete chat messages or disable private chat.
- **Participant list.** You can always see who has joined your video conference or webinar.

You may also be interested in reading our guide on how to help you to keep unwanted guests and crashers out of your video conferences.

**Screen sharing** is a useful- but also a sensitive- feature when it comes to information security. You want to be 100% sure that you are sharing what you think you are sharing. Digital Samba doesn't require any plugins for screen sharing, so you don't need to worry about installing something on your computer. When you want to share your screen, **consent for screen sharing is explicitly and unambiguously requested**, and you are presented with clear options to choose what you want to share. Our software also lets you preview what you are sharing anytime, which gives you the peace of mind that you are not sharing something private.

## Our commitment to data privacy and the GDPR

At Digital Samba, we take data privacy seriously, and we have taken extensive steps to ensure that we adhere to data privacy regulations, with a particular focus on the **General Data Protection Regulation (GDPR)**. Detailed information can be found on our data privacy and data security page.

## Cookies and tracking

We use cookies and other technologies to **improve and customise Digital Samba, our website and your experience**. A huge benefit is that it allows you to access and use Digital Samba without re-entering your username or password. It also helps us to understand the usage of our products and the interests of our users, which enables our team to create the best video conferencing experience for you. Detailed information can be found in Cookies and Tracking Notice.

## Dedicated to your security

Digital Samba opened for business when Skype wasn't even a verb yet. Over the years, we have adapted to the ever-shifting security landscape in the world of video conferencing, providing our customers with enterprise-level protection against actual and potential security threats. We have decades of experience, so you can rely on us to fight the good fight against malicious actors out there and keep your data and information safe.

## Want to talk about privacy & security in video conferencing?

Our security specialists at Digital Samba are happy to answer any questions you may have.