xtendx®
corporate media solutions

simplex Meeting

Security Factsheet

xtendx AG | Adlikerstrasse 246, CH-8105 Regensdorf
t +41 43 299 92 92 **e** support@xtendx.com **w** www.xtendx.com

15.10.2020

Index

1 Overview

This document describes the different encryption mechanisms of xtendx sessions, the list of personal data we store and lists the 3rd party providers we work with.

To be fully GDPR compliant we also sign Data Processing Agreements with concerned parties.

2 Data flow and encryption

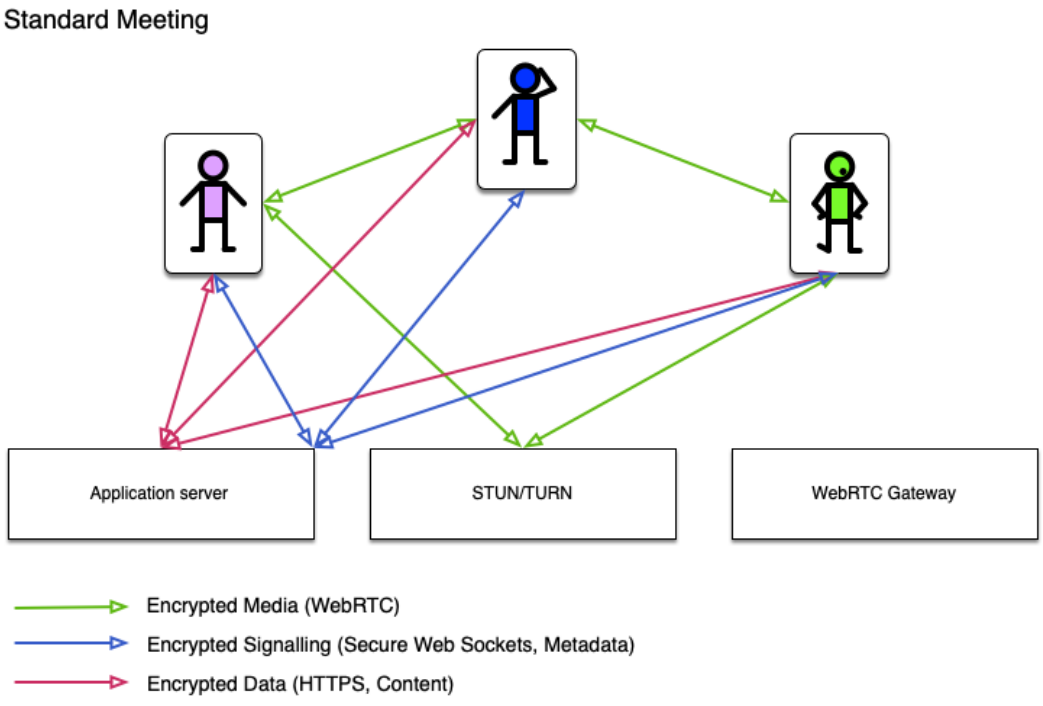
2.1 Meeting types and data flow

xtendx supports various meeting types. Each meeting type comes with special features, network requirements and security considerations.

2.1.1 Standard meeting

Participants in a standard meeting room communicate with end-to-end encrypted audio and video. In certain circumstances a direct peer-to-peer connection cannot be established. In these cases, a TURN server relies data between the participants. Documents and other information that are shared during the meeting are sent to the application server over HTTPS. The application server will create a meeting summary at the end of the meeting. Recording and dial-in is not possible.

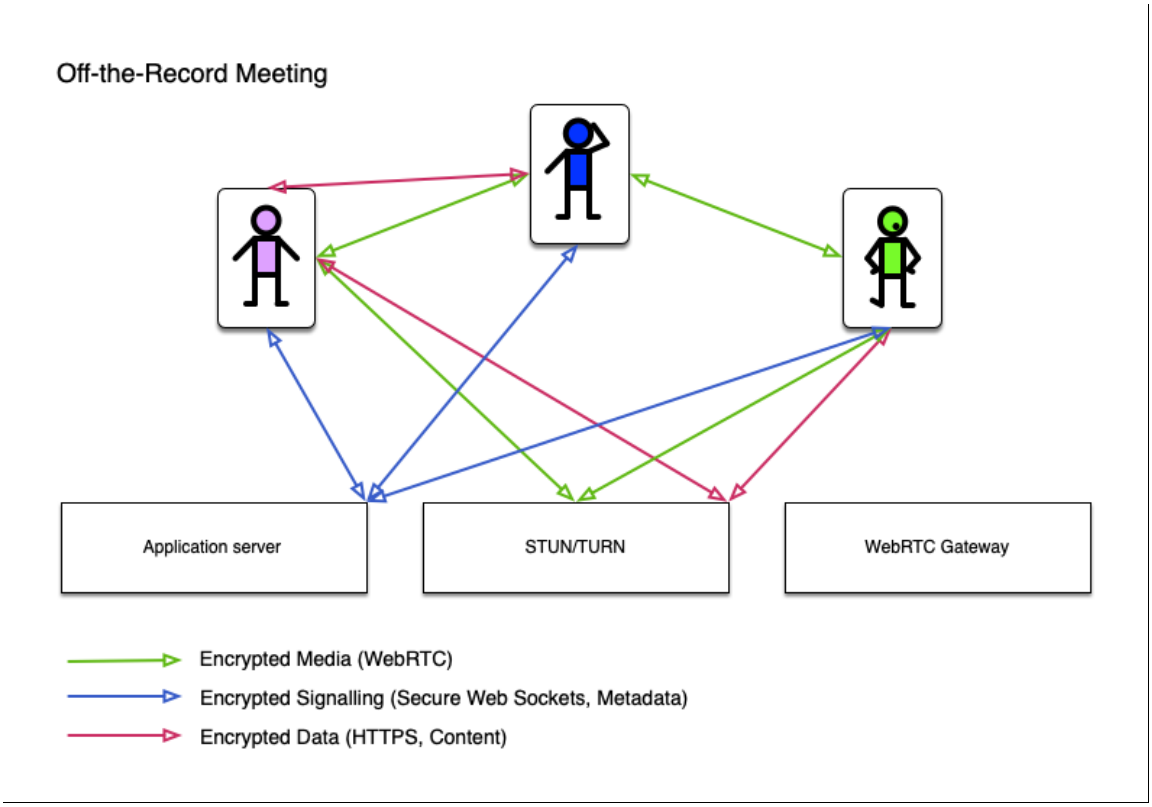
All signaling and content data sent between the web browsers and the servers is always 256-bit TLS 1.2 encrypted. All media (audio and video) is end-to-end encrypted with DTLS 1.2/SRTP encryption standards. The media remains end-to-end encrypted, even if the traffic is routed through a TURN server.



2.1.2 Off-the-record meeting

The Off-the-record (OTR) meeting is a variation of the standard meeting room. Audio and video are share in the same way. Documents and any other information shared during an OTR meeting are distributed among the participants through end-to-end encrypted data channels. Therefore, the xtendx system has no knowledge of the content of the meeting and does not produce a meeting summary. Recording and dial-in is not possible.

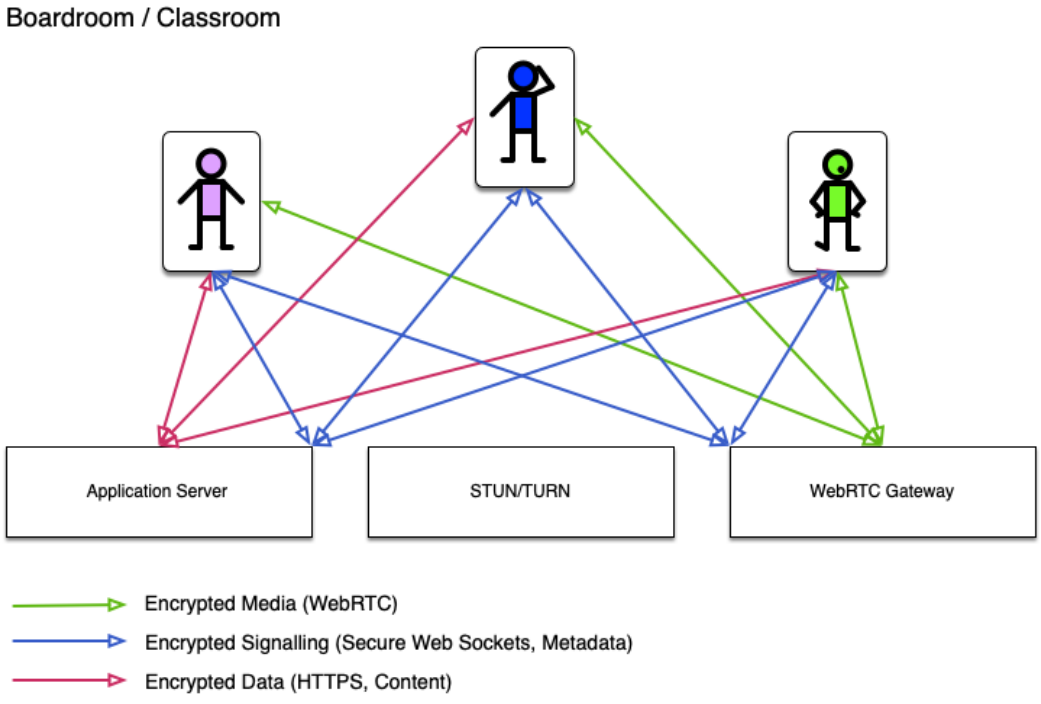
All signaling sent between the web browsers and the servers is always 256-bit TLS 1.2 encrypted. All media (audio and video) and data is end-to-end encrypted with DTLS 1.2/SRTP encryption standards. The media and data remain end-to-end encrypted, even if the traffic is routed through a TURN server.



2.1.3 Boardroom / Webinar (Classroom)

Boardroom and Webinar meetings are not end-to-end encrypted. Audio and video are always sent the SFU and distributed from there to the other participants of the meeting. The browser and the SFU communicate encrypted with each other, the SFU decrypts each video stream and encrypt it again for distribution. This allows for optional recording. All other data and information shared in a Boardroom or Webinar are stored on the application server for further use in meeting summaries. Recording and dial-in can be configured for these types of meetings.

All signaling and content data sent between the web browsers and the servers is always 256-bit TLS 1.2 encrypted. All media (audio and video) sent between the web browsers and the servers is always point-to-point encrypted with DTLS 1.2/SRTP encryption standards.



3 Data stored in Simplex Meeting

3.1 Overview

This section describes the personal data records stored in a White Label xtendx system and why the system stores this type of data.

3.2 Glossary

- **Meeting organizer**: Person with login credentials, authorized to schedule meetings.
- **Meeting participant**: Person attending a meeting.
- **Meeting admin:** The person who can create, edit, and delete accounts for session organizers, and has access to the support interface.

3.3 Stored data structures

3.3.1 Meeting organizer data stored in the system

This data is stored for as long as the account is paid for. Once the account becomes inactive (not paid anymore) the data is retained for 360 days in case the user decides to re-activate the account. After that the data, including "Meeting Data" is completely removed from the system.

The system only stores the most current values of these data sets.

Data set	**Required?**	**Reason for storing this data set**
Freely selectable account name	Yes	To identify an account by a name. Only applicable if the meeting organizer is also the account admin.
Company name	No	Only for billing purposes, will appear on invoices
First and last name of the meeting organizer	Yes	The name of the meeting organizer is shown in the meeting invitation that this meeting organizer sends through the system
Email address	Yes	The email address is used as the login username. It also acts as a reply-to address for meeting invitations and summaries, etc, sent by that user
Password	Yes	The password is stored slated and hashed, required to log in to the system
Description/comment	No	To add an internal comment to this customer.
Filter for network connections	No	The user can add network filters to prevent media traffic to be routed through internal VPN networks
Information about account-specific logo and colors	No	The user can upload a logo and define colors. The logo and colors are displayed during meetings organized by that account.
Preferred language of the user interface	Yes	The preferred language is stored to display the user interface in that language. It is also used to identify the language used in meeting invitations and summaries.
Timezone	No	Required to display additional timezones times in the meeting invitation
Permissions template for meeting	No	Permissions allow the user to restrict access to meeting room features.

Address book (List of email addresses)	Yes	Every email address used to send a meeting invitation is stored in the users address book. The address book is used for the "forward typing" feature when scheduling a meeting. Each email address can be deleted by the session organizer at any time. The email addresses in this address book are not used for any other purpose.
Documents	No	Documents uploaded by the meeting organizer. Can at any time be irrevocably deleted by the meeting organizer.
List of all planned and future meetings	Yes	To allow access to the meeting room. For details, see "Meeting data". Can at any time be irrevocably deleted by the meeting organizer.

3.3.2 Data of participant

The data is stored for as long as the "Meeting Data" is stored in the system, see below.

Data set	**Required?**	**Reason for storing this data set**
Name	Yes	The name will be visible to all other meeting participants of this meeting. It will also appear in the chat history next to any chat message that was sent. The name will also appear in the "Connection Statistics"
Email address	No	To send the meeting summary at the end of the meeting

If a participant participates in several meetings, no connection is made between the different meeting sessions. We do not track meeting participants across multiple meetings.

3.3.3 Meeting data

During the session all data filled in by participants (chat messages, uploaded documents, etc.) are stored. The meeting organizer has access to all these data, except the private notes of other participants in the "Past Meetings" section of the administration control panel. The meeting organizer can delete meetings and all related data at any time. The system does not automatically delete past meeting data except when configured accordingly.

After the meeting, if configured, the meeting data is automatically sent by email to all participants as a meeting summary.

Data set	**Required?**	**Reason for storing this data set**
Topic of the meeting	Yes	Required for the meeting invitation and summary as well as to identify meetings in the list of upcoming and past meetings
Meeting agenda	No	The agenda of the meeting.
Start date and time	Yes	Required to schedule a meeting and send a Calendar invitation.
Invited persons: list of email addresses	No	The list of participants are required to send meeting invitations and invitation updates.
Meeting password	No	The meeting can be protected by a password. If a password was set we require it to compare it with passwords entered by meeting participants prior to joining that meeting
Documents and files	No	Before and during the meeting the organizer and the participants can upload documents to be shared among all other participants. The system sends out a meeting summary with all the documents after the meeting to all meeting participants that have provided their email address.
Whiteboard drawings	No	Users can draw on the white board. These drawings are shared among all other participants. The system sends out a meeting summary with all the drawings after the meeting to all meeting participants that have provided their email address.
Chat messages	No	Users can chat in a group chat or individually between participants. The system sends out a meeting summary with the group chat after the meeting to all meeting participants that have provided their email address.
Meeting minutes	No	Users can write the meeting minutes during the meeting. The minutes are shared among all participants during the

		meeting. The system sends out a meeting summary with the meeting minutes after the meeting to all meeting participants that have provided their email address.
Private notes	No	The user can take private notes during the meeting. The system sends out a meeting summary including this private notes to the author of the notes, give that the author has provided an email address.

3.3.4 Connection statistics

During the meeting the system collects connection statistics of the participants. These connection statistics are stored exclusively for technical support purposes and are automatically deleted after 14 days.

- Operating system (name, version)
- Browser (vendor, type, version)
- Effectively used bandwidth and network statistics (round trip time, jitter, packet loss), every 15 seconds
- Type of connection (audio only or video)
- Connection errors
- Name of the participant, to easily identify the connection and find potential problems easily.

3.3.5 System logs

System and server logs are used exclusively for technical problem analysis and troubleshooting. The personal data (IP addresses, time, etc) are not automatically linked to data from meetings, participants or meeting organizers. The logs are deleted after 180 days.

3.3.6 Cookies, Locale Storage, Analytics and Data Analysis

Cookies and Locale Storage are used solely for system-related purposes (login, user settings, etc).

There are no analytics tools installed, we do not track users and/or analyse user generated data beyond what is absolutely necessary to provide the service. xtendx does not harvest data to generate added value for marketing purposes.

4 3rd parties

xtendx hosts all services on servers rented from Metanet AG (https://www.metanet.ch) or SWITCH whereby user data (except recordings) are always stored at Metanet. Metanet AG and SWITCH are

Swiss hosting providers and runs data centers exclusively within the physical borders of Switzerland.