KULTURSERVER

THE COMMUNITY FOR ART AND CULTURE

Appendix

Technical details for securing the video offer in the culturebase network

Berlin, September 2020

Stiftung kulturserver.de gGmbH

Geschäftsführung: Wolfgang Knauff
Amtsgericht Aachen HRB 10515

USt.-IdNr.: DE 230868040
Steuernr.: 127/602/52603

Mail: redaktion@kulturserver.de

Geschäftsstelle Berlin
Almstadtstraße 4
10119 Berlin
Tel.: +49 30 22667748
Fax: +49 241 33636

www.kulturserver.de

Geschäftsstelle Aachen
Lothringerstraße 23
52062 Aachen
Tel.: +49 241 33686
Fax: +49 241 33636

KULTURSERVER
THE COMMUNITY FOR ART AND CULTURE

In the following we would like to provide further detailed information on the implementation of the safeguarding of the video offer in the culturebase network.

The problem lies in the basic properties of all Internet-based services that are described by a link / URL and are therefore more or less freely and directly accessible at first. However, access is not always desired - for example for private data or for videos that are subject to a charge. What exactly the protection against unauthorized access looks like is explained in more detail below.

General description

Kulturserver uses infrastructure that is located in Germany. The servers are completely under the administration of our employees and no other external services / third-party providers need to be used. This means that Kulturserver has the security information at a glance and takes care of the continuous development of these servers.
The storage and delivery of the videos is secured via a server-side SecureLink module. Similar to DRM, it is a key-lock principle in which a link that is specific to each delivery is generated once, which is then valid for the transmission of the data.
This happens per data record, per user and at runtime - i.e. with a time limit. The link cannot simply be extracted from the code and used in a different way - or used without authorization for other videos by simply changing a video ID.

Detailed technical information

The NginX Secure module is used to secure the video offering
(http://nginx.org/en/docs/http/ngx_http_secure_link_module.html).

It is used to check the authenticity of requested links, to protect resources from unauthorized access and to limit the validity period of the links.

The validity of a requested link is checked by comparing the checksums transferred with the value calculated for the request. If a link has a finite lifespan and time has expired, the link is considered out of date. The service is made available in the $ secure_link variable.

A SecureLink consists of four components:

Service
https://u.culturebase.org
Path
e.g. /o/p/e/r/a/operation_k_i_alt_und_neu.2020.film.lang_de.mp4
Validity
a GET parameter with a Unix time stamp, e.g. t=1600170000 for a validity until 15.9.2020 13:40
Signature
a GET parameter to secure the other two values, e.g. sig=YDvO5x-6EmdAwO1MNIEiJA, for a description see below

The entire link in this example is:
https://u.culturebase.org/o/p/e/r/a/operation_k_i_alt_und_neu.2020.film.lang_de.mp4?t=1600170000&sig=YDvO5x-6EmdAwO1MNIEiJA

The streaming server can check the validity of this link without further knowledge of the user account or session:

- if the attached GET parameters are missing, the link is invalid
- if the timestamp is in the past, the link is out of date, i.e. invalid

The signature is necessary so that a user does not simply adjust the time stamp himself. The culturebase tool film7 calculates this from the path, the time stamp and a secret keyword that both film7 and the streaming server know:

- if the signature does not match the rest of the information, the link is invalid

Without knowing the secret key, a user cannot calculate a valid signature when the link is changed.

As a signature procedure, an MD5 sum is simply created using the three values (path, time stamp, key). The signature value is the Base64 representation of this MD5 sum.