CHANGE REQUEST

DASH-IF IOP	CR	0117	rev	-	Current version:	4.1

Status:		Draft		Internal Review	X	Community Review		Agreed

Title:	Support for SAND Interoperability
Source:	DASH-IF IOP
Supporting Companies:	TNO, Intel, Ericsson
Category:	**A** ***Date:*** 2018-01-08 *Use one of the following categories:* ***C*** *(correction)* ***A*** *(addition of feature)* ***B*** *(editorial modification)*

Reason for change:	Enable SAND interoperability in DASH-IF IOP
Summary of change:	The following additions are provided: • Modes defining subsets of SAND messages and mandatory SAND protocols to use for specific deployment environments • Normative behaviors on SAND message handling for DANE and DASH client • Security guidelines for SAND messages delivery • Procedures on DANE discovery for SAND
Consequences if not approved:	

Sections affected:	12 (new), 12.1 (new), 12.2 (new), 12.2.1 (new), 12.2.2 (new), 12.2.3 (new), 12.3 (new), 12.4 (new), 12.5 (new), 12.5.1 (new), 12.5.2 (new), 12.6 (new), 12.6.1 (new), 12.6.2 (new), 12.6.3 (new), 12.7 (new)
Other comments:	DASH-IF will seek to align the defined SAND modes with 3GPP.

Disclaimer:	This document is not yet final. It is provided for public review until the deadline mentioned below. If you have comments on the document, please submit comments by one of the following means: - at the github repository https://github.com/Dash-IndustryForum/IOP/issues (public at https://gitreports.com/issue/haudiobe/DASH-IF-IOP) - dashif+iop@groupspaces.com with a subject tag [UHD], or Please add a detailed description of the problem and the comment. Based on the received comments a final document will be published latest by the expected publication date below, integrated in a new version of DASH-IF IOP if the following additional criteria are fulfilled: - All comments from community review are addressed - The relevant aspects for the Conformance Software are provided - Verified IOP test vectors are provided
Commenting Deadline:	March 31st, 2018
Expected Publication:	June 30th, 2018

Add the following new references

[x1] ISO/IEC 23009-5:2017: "Information Technology — Dynamic adaptive streaming over HTTP (DASH) — Part 5: Server and network assisted DASH (SAND)"

[x2] DASH-IF Position Paper on SAND, available at: http://dashif.org/wp-content/uploads/2017/01/SAND-Whitepaper-Dec13-final.pdf

[x3] IETF RFC 6455: "The WebSocket Protocol".

[x4] Cross-Origin Resource Sharing, W3C Recommendation 16 January 2014, source: https://www.w3.org/TR/cors/.

[x5] The Web Origin Concept, A. Barth, Google, Inc., December 2011, RFC 6454

[x6] Mixed Content, W3C Candidate Recommendation, 2 August 2016, source: https://www.w3.org/TR/2016/CR-mixed-content-20160802/

[x7] XMLHttpRequest - Living Standard, source: https://xhr.spec.whatwg.org/

[x8] 3GPP TS 26.247 v15.0.0: "Transparent end-to-end Packet-switched Streaming Service (PSS); Progressive Download and Dynamic Adaptive Streaming over HTTP (3GP-DASH)".

Add the following new section

12 SAND Interoperability

12.1 Introduction

This clause addresses interoperability aspects and deployment guidelines for Server and Network Assisted DASH (SAND). Server and Network Assisted DASH (SAND) introduces messages between DASH clients and network elements or between various network elements for the purpose to improve efficiency of streaming sessions by providing information about real-time operational characteristics of networks, servers, proxies, caches as well as DASH client's performance and status. In particular, MPEG SAND aims to enable better cooperation between the DASH client and server operations, and provides the standardized interfaces toward realizing the following benefits for streaming services:

- Streaming enhancements via intelligent caching, processing and delivery optimizations on the server and/or network side, based on feedback from clients on anticipated DASH Segments, accepted alternative DASH Representations and Adaptation Sets, and requested bandwidth.
- Improved adaptation on the client side, based on network/server-side information such as cached Segments, alternative Segment availability, and network throughput/QoS.

SAND constitutes Part 5 of the MPEG DASH specifications, namely ISO/IEC 23009-5 [x1]. SAND has reached FDIS stage within MPEG as of June 2016. SAND reference architecture is depicted in Figure X. Within this architecture, the following four categories of messages, called SAND messages, are exchanged:

- Parameters Enhancing Reception (PER) messages that are sent from DANEs to DASH clients,
- Status messages that are sent from DASH clients to DANEs,

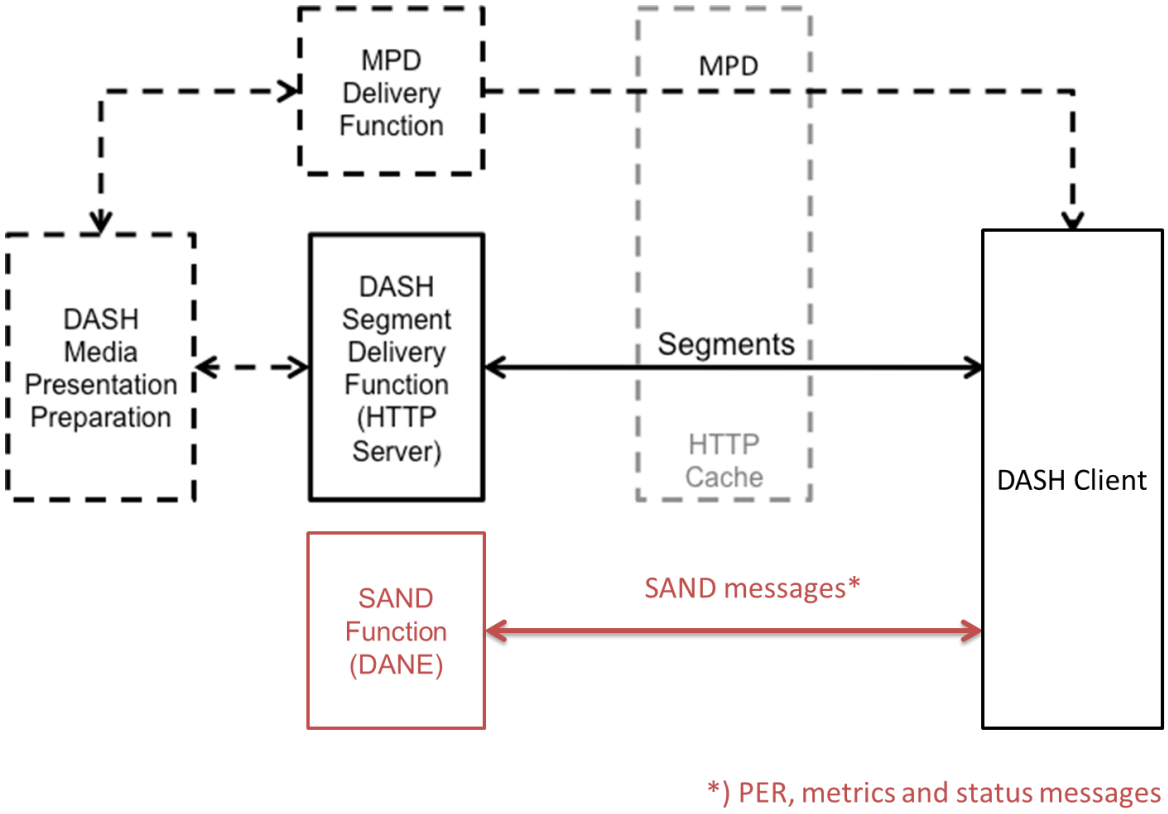

Figure X – SAND-augmented DASH reference architecture (taken from ISO/IEC 23009-5 [x1])

In December 2016, DASH-IF published a position paper on SAND [x2]. This paper presents several use cases and applications relevant for SAND, and also describes possible architectures and a few example workflows demonstrating how the various SAND features can help fulfill these use cases. As described in [x2], the SAND use cases can be grouped into two main buckets:

(a) DASH operation with proxy caches, including usages such as basic proxy caching, partial representation caching, MBMS-related proxy caching, HTTP proxy cache in a home gateway, next segment caching and multi-CDN offering.

(b) Consistent QoE/QoS for DASH users, including usages such as operator control of DASH in a cellular network, network assistance for DASH streaming and DASH clients collaboration within the home network

This clause describes the following:

- Modes defining subsets of SAND messages and mandatory SAND protocols to use for specific deployment environments
- Normative behaviors on SAND message handling for DANE and DASH client
- Security guidelines for SAND messages delivery
- Procedures on DANE discovery for SAND

12.2 SAND Modes

MPEG SAND defines message formats and exchange protocols between server, client, edge proxy and network elements toward enhancing streaming Quality of Experience (QoE). Based on these SAND message formats and protocols, this clause describes SAND modes, each of which comprises of a set of SAND messages and protocols that are required or recommended to be supported in a certain deployment environment.

12.2.1 Home gateway (or Consistent QoE/QoS)

This mode is intended for enabling content-aware network resource management to provide consistent QoE/QoS for DASH clients. Detailed use cases motivating this SAND mode can be found in clause 2.3 of [x2].

The mode comprises the following SAND messages:

- ClientCapabilities, as defined in clause 6.4.7 of ISO/IEC 23009-5 [x1]
- DaneCapabilities, as defined in clause 6.5.9 of ISO/IEC 23009-5 [x1]
- SharedResourceAssignment, as defined in clause 6.5.3 of ISO/IEC 23009-5 [x1]
- SharedResourceAllocation, as defined in clause 6.4.2 of ISO/IEC 23009-5 [x1]
- QoSInformation, as defined in clause 6.5.7 of ISO/IEC 23009-5 [x1]

DASH clients and DANEs supporting SAND functionality in the ‘Consistent QoE/QoS’ mode shall support the above SAND messages.

Note that this mode contains the same SAND messages as in the 3GPP SAND mode ‘Consistent QoE/QoS’ specified in clauses 13.4 and 13.8 of 3GPP TS 26.247 [x8], with the exception that it also contains the QoSInformation message.

The SAND status message *SharedResourceAllocation* shall follow the syntax and semantics in Table 4 of ISO/IEC 23009-5 [x1]. DASH clients sending the *SharedResourceAllocation* message shall include the bandwidth parameter. In addition, the SAND message common envelope shall contain the senderId parameter.

The SAND PER message *SharedResourceAssignment* shall follow the syntax and semantics in Table 16 of ISO/IEC 23009-5 [x1]. DASH clients receiving the *SharedResourceAssignment* message shall recognize the clientId and bandwidth parameters.

The SAND PER message *QoSInformation* shall follow the syntax and semantics in Table 22 of ISO/IEC 23009-5 [x1].

Example workflows for the SAND operation in the ‘Consistent QoE/QoS’ mode can be found in the DASH-IF position paper on SAND [x2] and also in clause 13.8 of 3GPP TS 26.247 [x8]. In this mode, the DASH client is expected to trust the information provided by the DANE regarding the available bandwidth. The information is especially valuable when the DASH client does not yet have a reliable estimation of the measured bandwidth, for instance when starting-up a new MPD, switching to a new server (e.g. different BaseUrl). Trusting the DANE will prevent slow quality ramp-up and other sub-optimal quality of experience effects. In addition, the buffer management logic may be less conservative under this mode in order to provide the intended consistent QoE. As a result, an existing DASH client implementation may need to be fine-tuned to make the best use of

this DANE-assisted mode, and adaption of the buffer management logic should be considered when necessary.

12.2.2 CDN edge (or Proxy Caching)

This mode is intended for enabling streaming enhancements via proxy caching. Detailed use cases motivating this SAND mode can be found in clauses 2.1 and 2.2 of [x2].

The mode comprises the following SAND messages:

- ClientCapabilities, as defined in clause 6.4.7 of ISO/IEC 23009-5 [x1]
- DaneCapabilities, as defined in clause 6.5.9 of ISO/IEC 23009-5 [x1]
- AnticipatedRequests, as defined in clause 6.4.1 of ISO/IEC 23009-5 [x1]
- AcceptedAlternatives, as defined in clause 6.4.3 of ISO/IEC 23009-5 [x1]
- DeliveredAlternative, as defined in clause 6.5.8 of ISO/IEC 23009-5 [x1]
- ResourceStatus, as defined in clause 6.5.1 of ISO/IEC 23009-5 [x1]
- MPDValidityEndTime, as defined in clause 6.5.4 of ISO/IEC 23009-5 [x1]

DASH clients and DANEs supporting SAND functionality in the 'Proxy Caching' mode shall support the above SAND messages.

Note that this mode contains the same SAND messages as in the 3GPP SAND mode 'Proxy Caching' specified in clauses 13.4 and 13.7 of 3GPP TS 26.247 [x8]. The message syntax and semantics described in clause 13.7 of TS 26.247 [x8] shall also apply for this SAND mode.

To realize partial representation caching, PER messages *ResourceStatus*, *DeliveredAlternative* and *MPDValidityEndTime* can be used to inform DASH clients about partially cached representations. Moreover, toward realizing next segment caching, DASH clients can inform the network (i.e., DANE) on anticipated DASH segments, acceptable alternative content, etc. leading to next segment caching, via the use of the status messages *AnticipatedRequests* and *AcceptedAlternatives.*

Example workflows for the SAND operation in the 'Proxy Caching' mode can be found in the DASH-IF position paper on SAND [x2] and also in clause 13.7.4 of 3GPP TS 26.247 [x8].

12.2.3 Network Assistance

The 'Network Assistance' mode is intended for enabling assistance from the network to DASH clients in the client rate adaptation and buffer fill procedures. Network assistance is part of the 'Consistent QoE/QoS' use cases in [x2]. The use case consists of providing the DASH client with better estimates of the short term throughput in a wireless network, so that DASH streaming sessions can better adapt to network conditions and avoid buffer under-run, hence stalling of audio/video playback. More details of the use case motivating this SAND mode can be found in clause 2.3.2 of [x2].

The 'Network Assistance' mode consists of two functions:

1) indicating to the DASH client the highest suitable media rate for the next segment download, based on the available Representations for the content item, and

2) indicating to the DASH client a temporary delivery boost for occasions when the content playback input buffer on the client risks suffering from under-run.

The second function is optional for the DASH client to indicate if it is needed or not.

The ‘Network Assistance’ mode includes a DANE discovery procedure as described in clause 12.7 DANE discovery. For 3GPP access the DANE discovery is also described in clause 13.3 of TS 26.247.

The DASH client shall initiate a Network Assistance session with the DANE handling the Network Assistance mode to make the network aware of its possible intended usage in advance of the first usage of the facility. The DASH client shall send the Session initiation message at a convenient stage in the process of preparing to receive media streaming content. When this takes place may be dependent on the nature of the application that streams media content items. The DASH client provides the DANE with the Media server IP address and the Media delivery port number. The DANE may in the response request the DASH client to set up a WebSocket connection to the DANE for all further Network Assistance communications in this session.

Once a Network Assistance session is active, the client may issue a Network Assistance call prior to fetching the next media segment from the server. The Network Assistance call consists of a single logical signalling exchange. This exchange with the DANE activates either the first of the above functions or a sequence of both functions; the second only if the DASH client was granted access to the function. If the client does not request a delivery boost, then the DANE omits the second function in the response to the DASH client.

The DASH client may make a call to the DANE before for each download of a media segment to get a recommendation of the highest suitable media rate, parameter Bandwidth, valid for the next-following period, parameter validityTime. The DASH client may use the value of the Bandwidth parameter as input to the rate adaptation algorithm in the selection of the media rate for the next media segment to be downloaded. The DASH client may make a call to the DANE both prior to downloading any media segment, i.e. in the initial phase of the media streaming session, as well as continuously during the media streaming session before every media segment download.

When the DASH client no longer requires Network Assistance facilities, it shall terminate the Network Assistance session. This could be the case for example when the playback of a streamed media content item is stopped, or the converse operation to that which occurred when the session was initiated.

The DANE supporting the ‘Network Assistance’ mode is out-of-band, i.e. not located in the media path. The DASH client shall send the NA SAND messages as the body of HTTP requests directly to the NA DANE, using the HTTP POST method to send a Network Assistance message to the DANE.

The ‘Network Assistance’ mode comprises the following SAND messages:

- ClientCapabilities, as defined in clause 6.4.7 of ISO/IEC 23009-5 [x1]
- DaneCapabilities, as defined in clause 6.5.9 of ISO/IEC 23009-5 [x1]
- SharedResourceAssignment, as defined in clause 6.5.3 of ISO/IEC 23009-5 [x1]
- SharedResourceAllocation, as defined in clause 6.4.2 of ISO/IEC 23009-5 [x1]

In addition, the following messages are defined, in 3GPP TS 26.247 [x8], for the Network Assistance mode:

- NetworkAssistanceInitiationRequest, as defined in clause 13.6 of TS 26.247 [x8]
- NetworkAssistanceInitiationResponse, as defined in clause 13.6 of TS 26.247 [x8]
- NetworkAssistanceTermination, as defined in clause 13.6 of TS 26.247 [x8]
- SegmentDuration, as defined in clause 13.6 of TS 26.247 [x8]
- DeliveryBoostRequest, as defined in clause 13.6 of TS 26.247 [x8]
- DeliveryBoostResponse, as defined in clause 13.6 of TS 26.247 [x8]

DASH clients and DANEs supporting SAND functionality in the 'Network Assistance' mode shall support the above messages.

The detailed description of the 'Network Assistance' mode can be found in clause 13.6 of 3GPP TS 26.247. The complete list of messages for this mode can be found in clause 13.6.5-6 of 3GPP TS 26.247 [x8], comprising both SAND messages as defined in ISO/IEC 23009-5 [x1], as well as messages defined specifically in 3GPP TS 26.247 [x8]. Example workflows for the SAND operation in the 'Network Assistance' mode can be found in the clause 13.6.7 of 3GPP TS 26.247 [x8].

12.3 Protocol Use

HTTP is the minimum mandatory transport protocol that is to be supported by DANEs and SAND-enabled DASH clients. In particular, the mandatory usages of HTTP for carrying SAND messages shall be according to Table 25 of ISO/IEC 23009-5 [x1].

In addition, DASH clients supporting SAND functionality as well as DANEs in the 'Network Assistance' and 'Consistent QoE/QoS' modes shall further support the WebSocket protocol specified in IETF RFC 6455 [x3], if the delivery of the DASH content occurs using HTTP over TLS (HTTPS). If HTTP over TLS (HTTPS) is not supported at a DASH client, then the support for the WebSocket protocol by the respective DASH client in the 'Consistent QoE/QoS' mode is recommended but not mandatory. Similarly, if HTTP over TLS (HTTPS) is not supported at a DANE, then the support for the WebSocket protocol by the respective DANE in the 'Consistent QoE/QoS' mode is recommended but not mandatory. As specified in ISO/IEC 23009-5 [x1], for advertising the SAND channel over WebSockets, the MPD shall contain a sand:Channel element whose @schemeIdUri is "urn:mpeg:dash:sand:channel:websocket:2016" and WebSocket URI in the @endpoint attribute.

12.4 Capability Exchange

On connection to a DANE, the DASH client shall send the status message ClientCapabilities in order to inform the DANE about the SAND mode(s) it supports. The DASH client shall use the messageSetUri parameter to indicate which SAND mode(s) it supports based on the following URNs:

- `http://dashif.org/guidelines/sand/modes/pc` to indicate support for the 'Proxy Caching' mode
- `http://dashif.org/guidelines/sand/modes/na` to indicate support for the 'Network Assistance' mode

- `http://dashif.org/guidelines/sand/modes/qoe` to indicate support for the 'Consistent QoE/QoS' mode

Depending on the SAND mode(s) supported by the DASH client, one or more of these URNs may be included in the ClientCapabilities message.

On connection to a DASH client, the DANE shall send the PER message DaneCapabilities in order to inform the DASH client about the SAND mode(s) it supports. The DANE shall use the messageSetUri parameter to indicate which SAND mode(s) it supports based on the following URNs:

- `http://dashif.org/guidelines/sand/modes/pc` to indicate support for the 'Proxy Caching' mode
- `http://dashif.org/guidelines/sand/modes/na` to indicate support for the 'Network Assistance' mode
- `http://dashif.org/guidelines/sand/modes/qoe` to indicate support for the 'Consistent QoE/QoS' mode

Depending on the SAND mode(s) supported by the DANE, one or more of these URNs may be included in the DaneCapabilities message.

If the DASH client has already discovered the DANE via the use of mode-specific FQDNs or PQDNs, the exchange of ClientCapabilities and DaneCapabilities messages shall not be performed on connection to a DANE.

12.5 SAND Message Handling Behaviors for DANEs and DASH clients

12.5.1 For DASH Clients

SAND Message	Actions	Nature
On `DaneCapabilities` and `SharedResourceAllocation` supported	Send `SharedResourceAllocation`	Mandatory
On `SharedResourceAssignment`	Select Representations for which the sum of the respective @bitrate values fit in the `@bandwidth` value of the `SharedResourceAssignment` message.	Optional
On `DaneCapabilities` and `AnticipatedRequests` supported	Send `AnticipatedRequests` with every future segment request.	Mandatory
On `DaneCapabilities` and `AcceptedAlternatives` supported	Send `AcceptedAlternatives` with any future segment requests.	Mandatory

On `MPDValidityEndTime`	If `@mpdUrl` is present, fetch MPD located at the `@mpdUrl` value before `@validityEndTime`.	Mandatory
	Else (`@mpd` is present by SAND specification), use `@mpd` as new MPD version when `@validityEndTime` has passed.	Mandatory

12.5.2 For DANEs

SAND message	Actions	Nature
On `SharedResourceAllocation`	1. Add client to the sharing strategy	Optional
	2. Update allocation strategy	Optional
	3. Send `SharedResourceAssignment` to clients in the sharing strategy	Mandatory
On `AnticipatedRequests`	Cache resources indicated by `AnticipatedRequests`	Optional
	Send `ResourceStatus` to signal available resources	Mandatory
On `AcceptedAlternatives`	Send `DeliveredAlternatives` in case DANE delivers an alternative segment rather than the requested segment	Mandatory
On WebSocket connection to DASH client in 'Consistent QoE/QoS' mode	If connection is QoS-enforced, send `QoSInformation`	Mandatory
On NetworkAssistanceInitiationRequest	Send NetworkAssistanceInitiationResponse	Mandatory
On NetworkAssistanceTerminationRequest	Send NetworkAssistanceTerminationResponse	Mandatory
On SegmentDuration and SharedResourceAllocation at Network Assistance mode	1. Derive a recommendation of bit rate, to include in Bandwidth, for next-following period, to include in validityTime	Mandatory
	2. Send SharedResourceAssignment including Bandwidth and validityTime	Mandatory
On DeliveryBoostRequest at Network Assistance mode	1. Determine whether delivery boost is granted, to be included in Status	Mandatory
	2. Send DeliveryBoostResponse including Status	Mandatory

12.6 Security guidelines for SAND messages delivery

MPEG-DASH is commonly delivered over HTTP. In clause 7.2 on HTTPS and DASH, the implications of using HTTP Over TLS for the delivery of DASH resources are discussed in general. This section provides additional considerations for deploying SAND using HTTP Over TLS.

12.6.1 HTTPS for SAND

MPEG-DASH SAND does not provide the mean to encrypt the content of the SAND messages. As a result, the use of HTTP Over TLS is recommended to protect agains man-in-the-middle attack. Indeed, HTTP over TLS ensures that only both end of HTTP transaction have access to the data exchanged preventing a rogue entity between the DASH client and the DANE to read the SAND messages.

SAND provides means for signaling different types of URI:

- URL of SAND messages in HTTP SAND Headers
- HTPP SAND Channel URI in the sand:Channel element in the MPD
- WebSocket SAND Channel URI in the sand:Channel element in the MPD

The MPEG-DASH SAND specification allows the use of the scheme 'https' for the URLs and the scheme 'wss' for the WebSocket URIs which both are their respective protocol identifier over TLS.

12.6.2 CORS aspects

Web browsers are by design to blocking cross-origin requests. These cross-origin requests occur when the user agent (the web browser) loads a resource on a certain origin (e.g. domain-a.com/index.html) while this resource points to other resources located on another origin (e.g. on domain-b.com). In this case, the web browser will block the request to other origina (here domain-b.com) for security reasons. For instance, the request to this other origin (domain-b.com) may be part of a phishing attack to capture sensitive information from the user.

However, it does not mean that all the cross-origin requests are malicious. Thereofre, the CORS specification [x4] defines a mechanism for a web browser to verifiy whether a cross-origin request is legitmate. The concept of origin is defined by [x5] in technical terms. An Origin is a tuple composed of a scheme, a host and a port of an URI. If two Origins are the same then they have the same scheme, host and port. Note that the scheme is the first part of the URI, e.g. "http", "https", which means that the same domain accessed via the "http" and the "https" schemes constitute two different Origins.

For implementation of SAND in web browser, one must then consider:

- Do the DANE serving SAND messages on HTPP and the DASH service have the same origin ?
    - If yes, there is no CORS issues. The DANE has the same origin as the DASH service.
    - If no, then the server hosting the DANE must be configured in such a way that it allows the user agents coming from at least the origin of the DASH service. It may allow more via for example a wildcard, see 5.1 Access-Control-Allow-Origin Response Header in [x4].
- Do the DANE signaled in the SAND Channel element by an HTTP URL and the DASH service have the same origin ?
    - If yes, there is no CORS issues. The DANE has the same origin as the DASH service.
    - If no, then the HTTP server hosting the DANE should be configured in such a way that it allows the user agents coming from at least the origin of the DASH service. It may allow more via a wildcard, see 5.1 Access-Control-Allow-Origin Response Header in [x4].

- Is a DANE signaled in the SAND Channel element by an WebScoket URI?
    - If yes, [x4] do not address cross-domain for WebSocket connections. At the time of writing, it appears that most popular web-browsers accept by default all cross-domain connections and no further configuration is required. However, the administrator of the DANE hosted on the WebSocket server may implement a domain validation using the Origin header passed on when the user agent connects to the WebSocket server. This way, user agents not coming from the domain of the DASH service can be immediately denied. Note that HTTP headers are easily changeable and this cannot constitue a method to authenticate legitimate DASH clients.
    - If no, then no further configuration is required.

Note that the CORS aspects related listed above are equivalent to deployments when the DASH service and the DASH resources (MPD and/or segments) are not located on the same domain.

12.6.3 Preventing mixed content

There are serveral advantages to serve the DASH service using HTTP Over TLS. Authenticating and/or authorizating user and clients while ensuring the secrecy of credential informantion is one of them. In order to maintain a high level of security for the entire service, the Mixed Content specification [x6] aims at defining the allowed and disallowed combinations of HTTP resources accessible via unsecure and secure protocols in a web page. That is, if a page is accessed via 'https' scheme then the web browser will block requests for resources accessible via 'http'. Note that there are exceptions to the strict blocage of mixed content for passive content such as images and videos provided as HTML element. However, these exceptions do not apply for browser-based DASH clients since these DASH clients fetch the video and audio segments via the XMLHttpRequest API [x7] for which any request is considered as active content.

For implementation of SAND in web browser, one must then consider:

- Is the DASH service served using HTTP over TLS?
    - If yes, then
        - a DANE in the SAND Channel element should be reachable either by a 'https' or 'wss' schemes which are the two secure protocols of respectively HTTP and WebSocket.
        - a SAND message URL provided in the SAND HTTP header should use the 'https' scheme.
    - If no, then there is no constraint of securing the exchange of the SAND messages according to the mixed Content specification.

12.7 DANE Discovery Procedures

The SAND specification [x1] provides the *sand:Channel* element in the MPD to inform the client about the location and method to communicate with the DANE. That method of DANE discovery may be used for DANEs that are in-band with respect to the media delivery path, i.e. when the MPD server may be aware of SAND functionality in the network.

When the DANE is out-of-band with respect to the media delivery path, as may be the case with the Consistent QoE/QoS DANE, a more generic method for DANE discovery may be used, namely using the DNS protocol. Toward this purpose, the UE needs a DANE Fully Qualified Domain Name (FQDN) or a Partially Qualified Domain Name (PQDN) for the DANE.

The use of FQDN would be specific to the operator or service provider policy. For example a 3GPP deployment of SAND uses the following FQDN for the DANE as defined in 3GPP TS 26.247 [x8]: "dane.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org". TS 26.247 also defines targeted DANE FQDNs for querying DANEs supporting specific SAND modes.

When receiving a DNS query on the PQDN “dane”, the DNS server shall respond with the information, including IP address, of the DANE or DANEs that are available to the UE for SAND functionality, according to any of the defined SAND modes.

A sub-domain “dane” is defined to be the PQDN where all DANEs are grouped logically. One or more DANEs that the network implements and provides for use by UEs in that network shall be accommodated logically under that sub-domain.

If only a single generic DANE is provided then the response shall provide the IP address where the generic DANE is reached.

Specific modes of DANE are identified as each being a sub-domain of the “dane” sub-domain, as follows:

- A Network Assistance DANE, if provided, shall be located at the PQDN “na.dane”.
- A Proxy-Caching DANE, if provided, shall be located at the PQDN “pc.dane”.
- A Consistent QoE/QoS DANE, if provided, shall be located at the PQDN “qoe.dane”;

If a specific mode of DANE is queried, using the specific sub-domain PQDN, then the response informs of the IP address of that mode of DANE only.