



Out-of-home Video
Advertising Bureau
Europe



OVAB Europe Standards

- Nr. 2 -

Service Level Agreements and Technical

Version 1.0 | January 2013

Dr. Frank Goldberg | Florian Rotberg

© OVAB Europe



DooH Service Level Agreements and Technical Standards

- To secure and guarantee the playout time of the advertisement, the DooH network, has to comply with certain service level and technical standards
- Aim: Customers can rely on the number of guaranteed spot playouts

Legal information

- Version 1.0
- Approved September 2012
- Ratified January 2013
- Review September 2013





Definition

- A certifiable network must consist of a minimum of 500 displays
- A professional operation has to guarantee a rate of 99% of error-free airtime (i.e. the maximum non-scheduled off-air-time is 1%)





For a successful certification the network provider has to prove that workflows and service level agreements guarantee the minimum of uninterrupted airtime

The service level agreements are:

- Detection of a display, playout-PC, or network connection failure within 30 minutes after the initial disruption (Mo.-Fr. 9:00 hrs - 17:00 hrs*)
- Reaction time after a failure (i.e. first attempt to eliminate the failure through remote maintenance by second level support) within 15 minutes (Mo.-Fr. 9:00 hrs - 17:00 hrs*)
- Recovery of the failure (i.e. failure elimination through remote maintenance by second level support) 2 hours (Mo.-Fr. 9:00 hrs - 17:00 hrs*)

* Has to be adapted to the definition of working days in certain regions



Continuation

- If disruption elimination through remote maintenance is not possible: Hardware exchange within 48 hours (Mo.-Fr.)
- Generate a failure report (ticket) by first level support within 1 hour after the detection of the failure
- Forwarding of failure reports (ticket) from first to second level support within 1 hour
- Closure of tickets by first level support within 1 hour after elimination of the disruption



SLA (with staff)

To comply with the aforementioned service levels operations can also be guaranteed through on-site staff. In this case the network operator has to prove through qualified documentation that a monitoring processes exists, that on-site staff is trained accordingly and instructed to resolve an incident

The documentation has to contain:

- Instructions for disruption detection
- Instructions for disruption elimination (incl. hardware change)
- Exemplary documentation for disruption elimination



SLA (technical)

If there is no possibility for a documentation and monitoring through on-site staff, the system has to be monitored via remote maintenance through a feasible technical solution (e.g. display controlling and readout with RS232 or similar port)

In this case the network operator needs to submit:

- Documentation of the monitoring solution (basic circuit diagram, data sheet)
- Examples for real-time or near-time systems monitoring (e.g. screenshots of the surveillance camera)
- Exemplary report of the monitoring system (e.g. reports of player-logs and display logs)



Connectivity

At any rate a central network connection with the following features is a basic requirement for the certification

- Transmission of content to a single player within 30 minutes
- Transmission of content to the complete network within 2 hours
- Possibility to query the current system status for every single system (player)
- Possibility of active transmission of heartbeats from every single system (player)
- Possibility to transmit player-log files



Professional Digital Signage Software

- Jitter-free display of common graphic and video formats
- Disruption free transitions between different contents
- Possibility to control individual systems as well as any user-defined group of systems
- User management system with administrative rights system
- Central content management system
- Active notification with the central system („heartbeat“)
- Documentation of log files for system controlling
- Documentation of log files for reporting
- Security concept incl. encrypted transmission of content



Professional Data Hosting

- Hosting of central components (e.g. Content Management System), digital signage software and all data records in suitable data centers
- Failure security of the central components and data records through admission control, energy and fire security and climate protection
- Adequate network performance through regular data backup
- Compliance with the Generally Accepted Data Processing Principles (GoD)
- Up to date anti virus and other IT security measurements
- Daily inspection of every data record for malware (e.g. Trojans, Viruses Spyware etc.) with up to date assessment and analysis procedures



Check List

- Data sheet of the implemented hardware
- Handbook of the implemented digital signage software
- Reporting of the last 12 months
- Ticket documentation of the last 12 months
- Service level agreements with external service providers
- Process and workflow documentation
- Random examination of the processes and workflows
- Inspection of the data center (optional)
- Sample check of the central monitoring and content management system
- Sample check of 5 systems respectively sites
 - Content error-free?
 - Content transmittable within 30 minutes/ 2 hours
 - Error reporting within the specified time



For more Information please contact OVAB Europe

Christine Koller
OVAB Europe Office Munich

Christine.Koller@ovab.eu
Phone: +49 89 2000416-17

OVAB Europe e.V. c/o
invidis consulting GmbH
Rosenheimer Str. 145e
81671 Munich / Germany