

Requirements

ID	Priority	Title	Description	Maximum score
A1	1. Critical	A1. Solution	The solution shall be a commercial off-the-shelf (COTS) system that is regularly updated and upgraded by the Participant to ensure that the solution adequately performs.	Knock-out
A2	1. Critical	A1. Solution	The solution shall have an appropriate, proven, reliable, secure and manageable architecture.	Knock-out
A3	1. Critical	A1. Solution	The solution shall be adequate and proportional to Eindhoven Airport's passenger numbers, flight numbers and operational peaks.	Knock-out
A4	1. Critical	A1. Solution	The solution shall be user-friendly and intuitive to use.	Knock-out
A5	1. Critical	A1. Solution	All central components of the solution, which are critical for the availability of the solution, i.e. a central server used by multiple work stations, shall be high-available and not be a single-point-of-failure.	Knock-out
A6	5. Question	A1. Solution	Describe an operating plan that details the operational processes proposed to ensure effective operation of the solution.	N/A
A7	5. Question	A1. Solution	Describe any resource requirements and dependencies required from EANV and handlers to operate the solution.	N/A
A8	5. Question	A1. Solution	Describe all of the hardware and infrastructure required for the proposed solution, including all engineering design work and integration design work, required to make the solution fully functional and meet all performance requirements.	N/A
A9	5. Question	A1. Solution	Provide detailed information and specifications of the hardware you propose, including images, photos and technical specifications.	N/A
A10	5. Question	A1. Solution	Describe the technical performance of the proposed solution. At least describe response times, boot times, barcode reading speeds, document reading speeds, print speeds.	N/A
A11	5. Question	A1. Solution	Describe what equipment will be located within EANV's core rooms and what cabinet/rack space is necessary to accommodate the system installation, operation, testing and maintenance.	N/A
A12	1. Critical	A2. Workstations and peripherals	The check-in workstation shall at least consist of the following components: - PC, monitor, mouse - Swipe keyboard (for passports and ID cards) - Boarding pass printer / receipt printer - Bag tag printer - Barcode scanner / boarding pass scanner	Knock-out
A13	1. Critical	A2. Workstations and peripherals	The service desk workstation shall at least consist of the following components: - PC, monitor, mouse - Swipe keyboard (for passports and ID cards) - Boarding pass printer / receipt printer - Barcode scanner / boarding pass scanner - Document printer	Knock-out
A14	1. Critical	A2. Workstations and peripherals	The gate workstation shall at least consist of the following components: - PC, monitor, mouse - Swipe keyboard (for passports and ID cards) - Boarding pass printer / receipt printer - 2x Boarding gate reader	Knock-out
A15	1. Critical	A2. Workstations and peripherals	The workstation at the baggage control room shall at least consist of the following components: - PC, monitor, mouse and keyboard - Bag tag printing - Document printing	Knock-out

Requirements

ID	Priority	Title	Description	Maximum score
A16	1. Critical	A2. Workstations and peripherals	The test workstation shall at least consist of the following components: - PC, monitor, mouse - Swipe keyboard (for passports and ID cards) - Boarding pass printer / receipt printer - Bag tag printer - Barcode scanner / boarding pass scanner	Knock-out
A17	1. Critical	A2. Workstations and peripherals	The (virtual) workstations at the back-office shall at least consist of the following components: - Virtual desktop or PC, monitor, mouse and keyboard - Document printing	Knock-out
A18	1. Critical	A2. Workstations and peripherals	The solution shall allow users to have multiple PPSs open on a workstation at any time and be able to switch instantly between these applications. All peripherals will be linked to the application that has focus.	Knock-out
A19	1. Critical	A2. Workstations and peripherals	The solution shall allow users to lock and unlock a computer and resume their work, without having to re-open/re-login again to applications the user had open before locking.	Knock-out
A20	1. Critical	A2. Workstations and peripherals	The workstations, as part of the solution, shall permit users to access additional local applications that are required for daily operation.	Knock-out
A21	1. Critical	A2. Workstations and peripherals	The solution shall provide integrated devices required for speedy and accurate identification of passengers. This shall include a document (passport / identity card) reader and barcode scanner, e.g. for boarding passes.	Knock-out
A22	1. Critical	A2. Workstations and peripherals	The solution shall support scanning of a barcode from a mobile phone, with a minimum performance of 20 boarding pass scans per minute.	Knock-out
A23	1. Critical	A2. Workstations and peripherals	The boarding pass printer shall have an auto cutter.	Knock-out
A24	1. Critical	A2. Workstations and peripherals	The bag tag printer shall have an auto cutter.	Knock-out
A25	1. Critical	A2. Workstations and peripherals	The workstation monitor is widescreen and has a minimum screen diagonal of 22 inch.	Knock-out
A26	2. High	A2. Workstations and peripherals	The solution should allow to access to back office functionality of PPSs through virtual desktop technology, such that (for example) a handling agent can access a PPS from his own corporate PC.	10
A27	2. High	A2. Workstations and peripherals	The virtual desktop setup shall allow for regular document printing from the PPS to a printer connected to the host work station, e.g. load sheets or other files.	10
A28	2. High	A2. Workstations and peripherals	The solution should minimise the amount of printer types required. A printer should be capable of both printing boarding passes and bag tags and can thus be configured to print either boarding passes or bag tags.	10
A29	2. High	A2. Workstations and peripherals	The solution should minimise the amount of printers at a workstation. E.g. a printer at a gate workstation should be capable of printing both boarding passes as receipts.	10
A30	2. High	A2. Workstations and peripherals	The bag tag printer should have a retainer that prevents the bag tag from falling after printing.	10
A31	2. High	A2. Workstations and peripherals	All peripherals should be compact and easily replaceable in case of a failure or upgrade.	10
A32	2. High	A2. Workstations and peripherals	The workstation's physical setup should be compact, secure and have neat cable management.	10
A33	3. Medium	A2. Workstations and peripherals	The gate work station should be expandable in the future, such that it also supports two self-boarding gates (in addition to the two boarding pass scanners / BGRs).	5
A34	3. Medium	A2. Workstations and peripherals	The solution should allow for upgrading local applications without the need for the Participant's intervention or re-certification.	5
A35	3. Medium	A2. Workstations and peripherals	EANV should have elevated permissions on all machines and computers for troubleshooting or analysis purposes.	5
A36	3. Medium	A2. Workstations and peripherals	The solution should allow for opening a local application while passing a computer identifier, e.g. host name, as a startup parameter.	5
A37	3. Medium	A2. Workstations and peripherals	The solution should allow for opening a web application while passing a computer identifier, e.g. host name, as a URL query parameter.	5
A38	3. Medium	A2. Workstations and peripherals	The solution should include document printers that support the ability for several workstations to share the same document printer.	5
A39	5. Question	A2. Workstations and peripherals	Describe the process of replacing a bag tag printer, a boarding pass printer, and a boarding pass scanner.	N/A

Requirements

ID	Priority	Title	Description	Maximum score
A40	5. Question	A2. Workstations and peripherals	Describe how the provided printing solution is reliable and economical. This is a necessity as the printer is used in a high-volume, operational environment.	N/A
A41	1. Critical	A3. Passenger Processing Systems	The solution shall support, but not limited to, the native Passenger Processing Systems of the following airlines: HV Transavia W6 Wizz Air W4 Wizz Air Malta OR TUI Netherlands TB TUI Belgium FR Ryanair RK Ryanair UK	Knock-out
A42	1. Critical	A3. Passenger Processing Systems	The solution shall support the DCS GoNow developed by Navitaire (Amadeus).	Knock-out
A43	1. Critical	A3. Passenger Processing Systems	The solution shall support the PPS SkySpeed developed by Navitaire (Amadeus).	Knock-out
A44	1. Critical	A3. Passenger Processing Systems	The solution shall support the DCS iPort developed by Res2.	Knock-out
A45	2. High	A3. Passenger Processing Systems	The solution should support the DCS eDCS developed by Aerocloud Systems.	10
A46	2. High	A3. Passenger Processing Systems	The solution should be certified to support, but not limited to, the native Passenger Processing Systems of the following airlines: PC Pegasus Airlines XQ Sun Express	10
A47	5. Question	A3. Passenger Processing Systems	Describe which Passenger Processing Systems are supported on your solution. Include details like whether the system is already connected to your solution, the type of connection used and method of access (including versions).	N/A
A48	5. Question	A3. Passenger Processing Systems	Describe how you collaborate directly with airlines, e.g. regarding deployment of DCS updates, and how we (as an airport) are actively involved in this collaboration.	N/A
A49	2. High	A4. Data, reporting and integration	The solution should have the capability to push a barcoded boarding pass data in real-time everytime when a boarding pass is scanned or printed. For example to an ActiveMQ topic and/or HTTP API. At least the following information is included: Flight date, flight number, booking reference, check-in sequence number, operation (e.g. BoardingPassPrint) and location (e.g. workstation name).	10
A50	2. High	A4. Data, reporting and integration	The solution should have the capability to push bag tag information in real-time everytime when a bag tag is printed. For example push this information to an ActiveMQ topic or HTTP API. At least the following information is included: Flight date, flight number, booking reference, check-in sequence number, bag tag number, bag weight, operation (e.g. BoardingPassPrint) and location (e.g. workstation name).	10
A51	2. High	A4. Data, reporting and integration	The solution should have an API to retrieve historical data in batch, such as platform usage data.	10
A52	2. High	A4. Data, reporting and integration	All log files related to the solution shall have a retention time of at least 30 days.	10
A53	5. Question	A4. Data, reporting and integration	Describe the information available through the standard reports that provide usage and describe the mechanism(s) for producing them.	N/A
A54	5. Question	A4. Data, reporting and integration	EANV would like to gather usage and statistical data associated to each PC and peripheral. Describe how this can be achieved.	N/A
A55	5. Question	A4. Data, reporting and integration	Describe how reporting data is stored within the system. Include details of how long the data is kept and how archived/historical data can be accessed/reported on.	N/A
A56	5. Question	A4. Data, reporting and integration	Describe the raw data available through the extract functionality and describe the mechanism(s) for retrieving this usage data.	N/A
A57	5. Question	A4. Data, reporting and integration	Describe the raw data available through the extract functionality and describe the mechanism(s) for retrieving this passenger flow data.	N/A
A58	5. Question	A4. Data, reporting and integration	Describe the frequency of how usage data and passenger flow data is available for extraction. Describe how often the data can be retrieved, e.g. the time elapsed from the most recent event.	N/A
B1	1. Critical	B1. Standards and compliance	The solution shall be fully CUPPS compliant (IATA RP1797 / ACI RP500A7 / A4A RP30.201).	Knock-out
B2	1. Critical	B1. Standards and compliance	The solution shall be compliant to IATA Technical Peripheral Specifications 2007 - 2012(formerly known as AEA).	Knock-out

Requirements

ID	Priority	Title	Description	Maximum score
B3	1. Critical	B1. Standards and compliance	The solution shall be fully compliant with the latest version of IATA Resolution 740 (Form of Interline Baggage Tag) and Recommended Practice 1740a (Baggage Tag Media Quality Guidelines).	Knock-out
B4	1. Critical	B1. Standards and compliance	The solution shall be fully compliant with the latest version of IATA Resolution 792 (IATA Bar Coded Boarding Passes).	Knock-out
B5	1. Critical	B1. Standards and compliance	The solution shall comply to the latest GDPR legislation (Currently General Data Protection Regulation 2016/679). Please describe how the solution conforms to the latest GDPR legislation.	Knock-out
B6	1. Critical	B1. Standards and compliance	Any personal data, which potentially is stored in debug files, log files or other data sources, shall be deleted 2 months after storage at the latest.	Knock-out
B7	2. High	B1. Standards and compliance	Any personal data, which potentially is stored in debug files, log files or other data sources, should be <u>automatically</u> deleted 2 months after storage at the latest.	10
B8	2. High	B1. Standards and compliance	The Participant is actively involved in the development of the CUPPS standard, by participating in IATA's CUSS & CUPPS task force.	10
B9	1. Critical	B2. IT infrastructure	The solution shall use the Layer 2 networking services provided by EANV.	Knock-out
B10	1. Critical	B2. IT infrastructure	The solution shall not contain any network switch provided by Participant.	Knock-out
B11	1. Critical	B2. IT infrastructure	The solution shall be able to connect to both local Passenger Processing Systems that are in the cloud or in private airline LANs.	Knock-out
B12	1. Critical	B2. IT infrastructure	The solution shall not require Wi-Fi/WLAN connectivity.	Knock-out
B13	1. Critical	B2. IT infrastructure	Internet access shall be provided by EANV (99,95% uptime).	Knock-out
B14	1. Critical	B2. IT infrastructure	If the Participants' solution requires on-premise servers, these servers shall be deployed on the hypervisor infrastructure of EANV.	Knock-out
B15	1. Critical	B2. IT infrastructure	If the Participants' solution requires on-premise virtual servers, these servers shall be within the following resource limits: 12 vCPU, 48GB RAM, 240GB HDD. Participant is allowed to dedicate these resources across one or more virtual machines.	Knock-out
B16	1. Critical	B2. IT infrastructure	If the Participants' solution requires on-premise virtual servers, any software license required to operate these virtual servers shall be included in the Participant's offer, including future upgrades and updates.	Knock-out
B17	1. Critical	B2. IT infrastructure	If the Participants' solution requires on-premise virtual servers, EANV will ensure these servers are backed up to two locations.	Knock-out
B18	2. High	B2. IT infrastructure	The solution should not require any local server at the premises of EANV.	10
B19	3. Medium	B2. IT infrastructure	The solution should provide an architecture that allows for efficiently connecting to the various PPSs.	5
B20	5. Question	B2. IT infrastructure	If the Participants' solution requires on-premise virtual servers, explain how you will manage and update these servers, such that these not become a technical debt over the span of this contract.	N/A
B21	5. Question	B2. IT infrastructure	Describe per airline how PPSs are connected to the proposed solution and how that connection is managed. Please provide a network architecture diagram of your proposed solution.	N/A
B22	2. High	B3. Performance	A CUPPS workstation is ready for use within 90 seconds after powering on the workstation.	10
B23	5. Question	B3. Performance	Describe expected response times for the solution, including but not limited to, print delay, scanning delay and user input delay.	N/A
B24	5. Question	B3. Performance	Describe the expected/estimated capacity of the offered solution in terms of passenger throughput.	N/A
B25	2. High	B4. Scalability	The solution should support new PPSs to be added with minimal effort. A new PPS should be added without the need for programmatic changes or a new software release.	10
B26	3. Medium	B4. Scalability	The solution should be capable of responding rapidly and easily to any unusual operations and peaks in passenger flow.	5
B27	5. Question	B4. Scalability	Describe how the system can be easily scaled, e.g. to support an increase of check-in desks or gates. Describe any limits of the proposed solution.	N/A
B28	5. Question	B4. Scalability	Describe your process of on-boarding a new PPS and the typical lead times.	N/A
B29	5. Question	B4. Scalability	Describe your process for how a new PPS can be connected to the solution. Highlight any costs associated with this process.	N/A

Requirements

ID	Priority	Title	Description	Maximum score
B30	5. Question	B4. Scalability	Describe what mobile functionality is available to both speed up and provide a more flexible approach to the check-in and boarding processes. Explain how the proposed solution can do this.	N/A
B31	1. Critical	B5. Sustainability	All delivered generic hardware (PC, monitor and document printer) shall be compliant with at least one of these certifications: TCO Certified, EPEAT Gold rating, Blue Angel or similar.	Knock-out
B32	1. Critical	B5. Sustainability	The PC monitor complies to energy label guidelines EU/2017/1369 and EU/2019/2013 and has the following energy label: - 21 - 24,5 inch: Energy label D - 24,6 - 27,9 inch: Energy label E - 28 - 30 inch: Energy label E - 30,1 - 32 inch: Energy label F This requirement can be adjusted throughout the term of the Agreement, in case the EU guidelines have been updated.	Knock-out
B33	1. Critical	B5. Sustainability	The monitor shall automatically switch off completely within a defined period after the connected computer has been shut down. When switched off, the monitor's power consumption shall not exceed 0.3 W.	Knock-out
B34	1. Critical	B5. Sustainability	The offered PCs shall be certified against the most recent Energy Star standard at the time of product launch.	Knock-out
B35	1. Critical	B5. Sustainability	The offered PCs shall be compatible with the most recent version of Advanced Configuration and Power Interface (ACPI) standard.	Knock-out
B36	1. Critical	B5. Sustainability	If the PCs have a built-in power supply unit (PSU), this PSU shall comply to 80 PLUS Gold standard or higher, or similar. This requirement does not apply to workstations that have an external PSU, such as micro form factor PCs and laptops.	Knock-out
B37	1. Critical	B5. Sustainability	All hardware is optimally configured with regard to power consumption and energy savings upon delivery and throughout the full term of the Agreement.	Knock-out
B38	1. Critical	B5. Sustainability	The Participant shall provide clear repair instructions after contract award, covering the recommended repair options for common product defects, whether or not these defects are covered by warranty.	Knock-out
B39	2. High	B5. Sustainability	The solution components should automatically switch to a low-power/standby mode when being idle for a configurable amount of time.	10
B40	2. High	B5. Sustainability	Participant should provide, within one month after delivery, a Life Cycle Assessment (LCA) for the delivered boarding pass and bag tag scanners and printers, excluding accessories. The LCA should include at least the product carbon footprint in CO ₂ equivalents, based on the GHG Protocol Product Standard or equivalent, broken down by raw materials, production, downstream transport and use phase. Where available, manufacturer LCAs based on ISO 14040/14044 should be used. A product lifetime of 5 years should be used.	10
B41	2. High	B5. Sustainability	The Participant should minimize the amount of packaging upon initial delivery of the hardware.	10
B42	3. Medium	B5. Sustainability	The offered boarding pass printers should be certified against the most recent Energy Star standard at the time of product launch.	5
B43	3. Medium	B5. Sustainability	The offered bag tag printers should be certified against the most recent Energy Star standard at the time of product launch.	5
B44	3. Medium	B5. Sustainability	The offered PCs should be repairable throughout its lifetime. Spare parts should be available for at least five years after its manufacturer stopped producing the PCs.	5
C1	1. Critical	C1. Implementation	The Participant shall appoint a capable project manager to take responsibility for delivering the solution. This Project Manager shall also have overall responsibility for the detailed planning, phasing and coordination of the entirety of the on-site works, including logistics, site-coordination and all associated permits.	Knock-out
C2	1. Critical	C1. Implementation	The Participant shall assemble a capable project team that shall have the right set of competences for delivering the solution.	Knock-out

Requirements

ID	Priority	Title	Description	Maximum score
C3	1. Critical	C1. Implementation	The Participant's project manager and teams shall collaborate with the EANV appointed project manager, all other consultants, sub-contractors and suppliers as necessary to ensure an integrated approach to the planning and implementation of the works. They shall deliver, install, commission and test the solution in accordance with the EANV project manager's overall accepted schedule.	Knock-out
C4	1. Critical	C1. Implementation	The Participant shall provide their own software in the latest software version at the time of installation.	Knock-out
C5	5. Question	C1. Implementation	Describe the implementation plan, including key milestones, timescales, assumptions and risks.	N/A
C6	5. Question	C1. Implementation	Describe the organisational structure that will be in place throughout implementation, including a description of the competences of all people involved throughout the implementation.	N/A
C7	5. Question	C1. Implementation	Describe any resource requirements and dependencies required from EANV and/or it's handlers to deliver the solution.	N/A
C8	5. Question	C1. Implementation	Describe the equipment and tools, if any, required to deliver the solution.	N/A
C9	1. Critical	C2. Acceptance and go-live	The Participant shall develop an acceptance plan that is approved by EANV at least 14 days prior to the test date. The plan shall at least address all requirements identified in the Programme of Requirements and test all Participant supplied hardware and software components.	Knock-out
C10	1. Critical	C2. Acceptance and go-live	The solution shall be fully delivered, implemented and accepted by 1 June 2027 at the latest.	Knock-out
C11	1. Critical	C2. Acceptance and go-live	The Participant will provide all materials and test equipment for carrying out the acceptance plan.	Knock-out
C12	1. Critical	C2. Acceptance and go-live	Any specified item that does not satisfy the requirements shall be replaced, upgraded, or added by the Participant as necessary to correct the noted deficiencies. After correction of a noted deficiency, re-testing shall be performed to verify the effectiveness of the corrective action.	Knock-out
C13	1. Critical	C2. Acceptance and go-live	The Participant's offered solution shall undergo a penetration test, performed by an independent third party appointed by EANV. The results of this penetration test is part of the acceptance criteria, such that no Critical or High findings may be open for acceptance.	Knock-out
C14	1. Critical	C2. Acceptance and go-live	The Participant shall ensure a focused period of support in the first 10 days of operation, in order to address and resolve any question and/or issue promptly and adequately.	Knock-out
C15	2. High	C2. Acceptance and go-live	The High Level Design documentation and Low Level Design documentation should be delivered by 1 March 2027 at the latest.	10
C16	2. High	C2. Acceptance and go-live	A single CUPPS workstation, for exploration, testing and pentesting purposes, should be delivered by 1 March 2027 at the latest.	10
C17	5. Question	C2. Acceptance and go-live	Describe how you would ensure this focused period of support during the first 10 days of operation.	N/A
C18	5. Question	C2. Acceptance and go-live	Describe the process for testing and accepting new applications and upgrades on the solution prior to deploying it to the live environment.	N/A
C19	5. Question	C2. Acceptance and go-live	Describe the process for testing new and replacement hardware on the solution prior to deploying it to the live environment.	N/A
C20	1. Critical	C3. Training, materials and manuals	The proposed solution shall include adequate training of key personnel. This should include but not be limited to, field service engineers, system administrators and operational staff.	Knock-out
C21	1. Critical	C3. Training, materials and manuals	The Participant shall provide training materials required to operate and maintain the solution prior to acceptance.	Knock-out
C22	1. Critical	C3. Training, materials and manuals	The Participant shall provide copies of all operational and maintenance manuals free of charge. These manuals shall be in electronic format.	Knock-out
C23	1. Critical	C3. Training, materials and manuals	The Participant shall provide updated versions of all manuals and documentation free of charge and shall actively notify EANV about this update.	Knock-out
C24	1. Critical	C3. Training, materials and manuals	The Participant shall provide training to key personnel at the premises of EANV on dates to be mutually agreed.	Knock-out
C25	2. High	C3. Training, materials and manuals	The solution shall include initial on-site training prior to system acceptance testing for system administrators and end users.	10
C26	5. Question	C3. Training, materials and manuals	Describe a training plan for the training of all key personnel.	N/A
C27	1. Critical	C4. Offering	The solution shall include all the necessary licenses and any third party licenses that are required to make the solution fully operational.	Knock-out

Requirements

ID	Priority	Title	Description	Maximum score
C28	2. High	C4. Offering	Virtual desktop based back-office CUPPS should be licensed concurrently, e.g. via a license pool. This should minimize the amount of required licenses as not all back-office virtual desktops are in use at the same time.	10
C29	5. Question	C4. Offering	Provide a detailed breakdown of all options supported by the solution, e.g. peripheral options, and their associated costs. This is to ensure that EANV is able to select the most cost effective configuration of the solution.	N/A
C30	5. Question	C4. Offering	Describe any additional costs that may occur with respect to using your proposed solution that are outside of your commercial proposal.	N/A
D1	1. Critical	D1. Service Level Agreement	The proposed Service Level Agreement (SLA), as part of the solution, shall include clearly defined, measurable service levels and key performance indicators (KPIs) covering the proposed maintenance and support contract.	Knock-out
D2	1. Critical	D1. Service Level Agreement	Any scheduled downtime of the solution shall be fully planned and approved by EANV in advance.	Knock-out
D3	1. Critical	D1. Service Level Agreement	The solution shall have a minimum availability of 99.9% per calendar month, with a 24/7 service window excluding agreed maintenance windows.	Knock-out
D4	1. Critical	D1. Service Level Agreement	The Service Level Agreement shall define at least the following four incident severity levels: P1 – Critical: A major service disruption or outage affecting business-critical passenger processing operations, multiple operational areas, or a substantial number (3 or more) of workstations or peripherals, with immediate operational impact. P2 – High: A disruption affecting one or more business-critical workstations, peripherals, interfaces, or functions, where operations can continue only through workaround procedures or with reduced capacity. P3 – Medium: Degraded performance, intermittent errors, or a partial loss of functionality that does not have an immediate operational impact and for which normal operations can continue. P4 – Low: General requests, minor issues that do not affect live operations (if handled and resolved in-time) and can be handled through normal planning and prioritisation.	Knock-out
D5	1. Critical	D1. Service Level Agreement	The Participant shall meet the following minimum incident response and resolution targets: P1 - Response ≤ 30 minutes, resolution ≤ 4 hours P2 - Response ≤ 1 hour, resolution ≤ 8 hours P3 - Response: ≤ 1 day, resolution ≤ 5 days P4 - Response: ≤ 2 days, resolution ≤ 7 days Service window: 24/7	Knock-out
D6	1. Critical	D1. Service Level Agreement	The Participant shall meet the following minimum service and change request targets: Configuration update: response ≤ 1 business day, resolution ≤ 5 business days Service request: response ≤ 1 business day, resolution ≤ 5 business days Change: response ≤ 2 business day, delivery of plan of approach ≤ 10 business days Participant may include additional/different service request types in its SLA proposal.	Knock-out
D7	1. Critical	D1. Service Level Agreement	A certificate update, a URL change, the addition of a browser-based application are all considered configuration updates and shall be handled as such.	Knock-out
D8	1. Critical	D1. Service Level Agreement	The Participant shall provide a documented escalation procedure including 24/7 contact details.	Knock-out
D9	1. Critical	D1. Service Level Agreement	The Participant shall clearly define responsibilities between the Participant, EANV TS&FM team and EANV D&IT Team for operation, maintenance, security and support.	Knock-out
D10	1. Critical	D1. Service Level Agreement	The Participant shall actively support all proposed hardware and peripherals for the full contract period (including extensions).	Knock-out

Requirements

ID	Priority	Title	Description	Maximum score
D11	1. Critical	D1. Service Level Agreement	The three lines of support are defined as follows, to which the Participant agrees: 1st line support: The initial support function responsible for receiving, registering, prioritising and coordinating incidents, service requests and questions relating to the CUPPS solution. 1st line support includes first diagnosis, basic troubleshooting, user assistance, replacement of easily replaceable peripherals where this is within EANV's agreed responsibilities, and escalation to 2nd line support where the incident or request cannot be resolved within the agreed scope, skills, access rights or working hours of EANV's TS&FM and D&IT teams. 2nd line support: The specialist operational and technical support function responsible for incidents, service requests and maintenance activities that cannot be resolved by 1st line support but do not require changes to, or expert development-level intervention in, the CUPPS software platform. 2nd line support includes deeper functional and technical analysis, configuration support, coordination of hardware or peripheral issues, support for integrations and operational workarounds, preventive maintenance activities, and escalation to 3rd line support where product-level expertise, software maintenance or development authority is required. 3rd line support: The expert product and platform support function responsible for resolving incidents, problems and changes that require in-depth knowledge of, and direct control over, the CUPPS software platform. 3rd line support includes product-level troubleshooting, software defect analysis and correction, release and patch support, configuration or maintenance actions that affect the core CUPPS platform, and support for structural improvements to the solution.	Knock-out
D12	1. Critical	D1. Service Level Agreement	First line of support shall be provided by the local teams of EANV (Department of Technical Services and Facility Management + Department of Digital & IT).	Knock-out
D13	1. Critical	D1. Service Level Agreement	The Participant may rely on the performance of local EANV staff for incidents. However, this shall be limited to the working hours of the respective local team, limited to activities that can only be done on-premise, and limited to 4 hours for P1 incidents, and limited to 1 hour for P2/P3/P4 incidents. After this time local staff shall be released from the incident and Participant shall resolve the incident independently. At all times the Participant is responsible for managing and coordinating the incident response.	Knock-out
D14	1. Critical	D1. Service Level Agreement	If an incident or service request cannot be resolved remotely, the Participant may request support from local EANV staff to help resolve the issue. Such support is provided on a best-effort basis and does not defer, reduce, or otherwise modify the Participant's SLA obligations.	Knock-out
D15	1. Critical	D1. Service Level Agreement	If an incident or service request cannot be resolved remotely, and EANV is unable to provide local staff support, the Participant shall dispatch suitably qualified personnel to the site. Any costs associated with on-site support required to resolve incidents shall be included in the SLA fees. Costs for on-site support related to service requests shall be agreed in advance between EANV and the Participant.	Knock-out
D16	1. Critical	D1. Service Level Agreement	First line of support shall be limited to standard operating procedures and troubleshooting steps for which Participant have shared manuals/instructions with EANV. These procedures shall have a duration of less than 30 minutes and shall not contain tasks that require specific skills or certifications, and can be performed by . Any support task that takes more than 30 minutes or requires specific skills is considered 2nd line support.	Knock-out
D17	1. Critical	D1. Service Level Agreement	The SLA shall include a preventive maintenance plan in order to keep all system component in optimal condition and to minimize the amount of corrective maintenance.	Knock-out
D18	1. Critical	D1. Service Level Agreement	The Participant may rely on the performance of local EANV staff for easy preventive maintenance tasks that have a daily, weekly, bi-weekly or monthly frequency. The total time required on these tasks shall not exceed 8 hours per month.	Knock-out
D19	1. Critical	D1. Service Level Agreement	Any preventive maintenance tasks, with a frequency lower than monthly, shall be performed by Participant's staff.	Knock-out
D20	1. Critical	D1. Service Level Agreement	The Participant will perform a full system health check at least once every six months. This health check shall be performed in-person, on-site.	Knock-out

Requirements

ID	Priority	Title	Description	Maximum score
D21	1. Critical	D1. Service Level Agreement	The Participant will actively advise EANV on what spare parts to have on stock throughout the full term of the agreement.	Knock-out
D22	2. High	D1. Service Level Agreement	The SLA should include a pro-active, remote monitoring service including pro-active intervention in case an issue is detected.	10
D24	5. Question	D1. Service Level Agreement	Describe the support process and the organisational structure of the support (1st, 2nd & 3rd line) supplied. Demonstrate that you incorporate the working hours and expertise of the EANV teams that are involved in 1st line support.	N/A
D25	5. Question	D1. Service Level Agreement	Describe how you differentiate the processing of simple service requests and more complex/impactful service requests.	N/A
D26	5. Question	D1. Service Level Agreement	Describe the preventive maintenance plan on a detailed level, describing task, frequency and responsibility. The plan should be concise, and proportional.	N/A
D27	5. Question	D1. Service Level Agreement	Describe the process for warranty and non-warranty replacements and repairs throughout the contract period (including extensions).	N/A
D28	5. Question	D1. Service Level Agreement	Describe the spare part strategy you would advise to EANV for this agreement.	N/A
D29	1. Critical	D2. Business Continuity	The solution shall include automated backups of all relevant system data.	Knock-out
D30	1. Critical	D2. Business Continuity	The solution shall define and meet the following recovery objectives: Recovery Time Objective (RTO): maximum 4 hours Recovery Point Objective (RPO): maximum 8 hours	Knock-out
D31	1. Critical	D2. Business Continuity	The Participant shall define backup retention periods and procedures for restoring historical data. Upon request, these procedures will be shared with EANV.	Knock-out
D32	2. High	D2. Business Continuity	The solution should incorporate a proven disaster recovery architecture.	10
D33	5. Question	D2. Business Continuity	Describe your disaster recovery plan that outlines the various processes that will be put in place should a disaster happen.	N/A
D34	5. Question	D2. Business Continuity	Describe your incident management process, including governance, escalation and major incident management.	N/A
D35	1. Critical	D3. Account Management	The Participant shall appoint a capable account manager that remains engaged throughout the contract period (including extensions), who is responsible for following up on any matter that may require escalation and joint resolution.	Knock-out
D36	1. Critical	D3. Account Management	The Participant shall participate in periodic service review meetings.	Knock-out
D37	2. High	D3. Account Management	The account manager shall frequently report about (at least) the performance of the contract, SLA KPIs, on-going incidents/problems, software vulnerabilities, every quarter by means of a written report.	10
D38	5. Question	D3. Account Management	Describe the on-going account management, support and service delivery management for the solution.	N/A
D39	2. High	D4. Monitoring and alerting	The solution shall send a notification when the toner cartridge of a document printer is almost empty, containing the printer name/location and cartridge model.	10
D40	2. High	D4. Monitoring and alerting	The proposed solution should include real-time, remote monitoring platform that provide insight in the state of the system, including but not limited to, peripheral connection state, paper levels etcetera. This monitoring tooling should be available to EANV and its field support staff.	10
D41	2. High	D4. Monitoring and alerting	The solution should be capable of actively sending notifications for a configurable set of alerts. It should at least be possible to send these notifications via e-mail.	10
D42	2. High	D4. Monitoring and alerting	The proposed solution can be monitored through standard monitoring interfaces, e.g. SNMP or an API, in order to include the solution into EANV's central monitoring and alerting system.	10
D43	3. Medium	D4. Monitoring and alerting	The solution should monitor the validity of client certificates used for authentication for airline systems, and alert when the certificate is about to expire.	5
D44	3. Medium	D4. Monitoring and alerting	All technical texts, e.g. error messages, log texts etcetera, should be in the English language and non-generic, i.e. properly describing the actual occurrence.	5
D45	5. Question	D4. Monitoring and alerting	Describe how support personnel can access real-time monitoring information.	N/A
D46	5. Question	D4. Monitoring and alerting	Describe what components of the solution can be monitored through monitoring interfaces like SNMP.	N/A

Requirements

ID	Priority	Title	Description	Maximum score
D47	1. Critical	D5. Product life-cycle	When the Participant releases a new version of its software during the contract period (including extensions), this new version shall be made available to EANV as part of on-going support without additional costs.	Knock-out
D48	1. Critical	D5. Product life-cycle	The solution, including all its components, shall be actively supported by its respective manufacturer throughout the contract period (including extensions). In case this requires software upgrades throughout the contract period, this is considered as part of on-going support. No additional costs shall be charged.	Knock-out
D49	1. Critical	D5. Product life-cycle	The Participant shall follow a formal change management process including impact analysis, rollback procedures and approval by EANV.	Knock-out
D50	2. High	D5. Product life-cycle	New generations of the solution hardware should be made available to EANV. EANV should not be limited to the initially provided hardware throughout the contract period (including extensions). EANV should be able to take advantage of new technology innovations.	10
D51	2. High	D5. Product life-cycle	New hardware, which becomes available throughout the contract period (including extensions) should be backwards compatible to the initially proposed solution. For example, new generation printers must be compatible with the originally supplied workstation and related (software) systems.	10
D52	3. Medium	D5. Product life-cycle	Throughout the term of the contract, EANV prefers to buy hardware expansions and spare parts from Participant. However, EANV should be permitted to purchase hardware and peripherals from other vendors. If this hardware is identical to the existing install base, Participant should fully adopt and support this hardware into its solution.	5
D53	5. Question	D5. Product life-cycle	Describe the Participant's change management and release management processes for the proposed solution. The description should include, where applicable, the governance structure, change advisory or control board, approval process, testing approach, release planning, communication, rollback procedures, and documentation.	N/A
D54	5. Question	D5. Product life-cycle	Provide details of how you engage and manage your customer base to input and develop the products included in your solution.	N/A
D55	5. Question	D5. Product life-cycle	Describe any formal mechanisms you organize regarding governance, meetings and input as part of product development lifecycle, e.g. user groups.	N/A
D56	5. Question	D5. Product life-cycle	Explain the planned life-cycle of the proposed solution and its components, including when it was launched, when its obsolescence is planned, and what the plans are for its replacement. Tailor this explanation to this project.	N/A
D57	5. Question	D5. Product life-cycle	Describe the plans to develop the solution over the next 5 years and provide a clearly defined roadmap. This shall include details of how the Participant will guarantee the product has support and does not become obsolete.	N/A
E1	1. Critical	E1. Cyber Security	The solution shall comply to the Security Annex of EANV throughout the full contract period including extensions.	Knock-out
E2	1. Critical	E1. Cyber Security	Work stations shall have an automatic, configurable time-out function to ensure a computer is automatically locked after a configurable timeout.	Knock-out
E3	1. Critical	E1. Cyber Security	The solution shall be designed in accordance to the concepts of zero-trust and least privilege.	Knock-out
E4	1. Critical	E1. Cyber Security	The solution shall be segmented into multiple VLANs in accordance to industry best practices, and up to agreement by EANV. Inter-VLAN traffic shall be inspected by a next-generation firewall.	Knock-out
E5	1. Critical	E1. Cyber Security	The solution should allow for support the integration of a handler's identity provider, based on common standards (at least Entra ID, OAuth and SAML2.0). This should enable every handler's agent to reuse their corporate credentials for logging in to a workstation.	Knock-out
E6	1. Critical	E1. Cyber Security	All network traffic between the local networks at EANV's premises and the Participant's (or third parties acting on behalf of the Participant) external networks shall be encrypted in accordance to modern cryptography standards.	Knock-out
E7	1. Critical	E1. Cyber Security	All components of the solution shall be hardened in accordance to industry best practices and benchmarks, e.g. CIS.	Knock-out
E8	1. Critical	E1. Cyber Security	The solution should allow for creating multiple user roles that have different access levels.	Knock-out
E9	1. Critical	E1. Cyber Security	The solution shall incorporate modern security levels and standards and not rely on outdated or inappropriate security measures.	Knock-out
E10	1. Critical	E1. Cyber Security	The solution shall implement encryption-at-rest where possible. At least all hard drives of local PCs shall be encrypted.	Knock-out
E11	1. Critical	E1. Cyber Security	The solution shall be monitored 24/7 for (potential) security incidents and/or breaches. Alarms shall be actively acted upon.	Knock-out

Requirements

ID	Priority	Title	Description	Maximum score
E12	1. Critical	E1.Cyber Security	The solution shall be frequently scanned for vulnerabilities, using automated tooling. Vulnerabilities will be resolved in accordance to the requirements as described in the Security Annex.	Knock-out
E13	2. High	E1.Cyber Security	The firewall, segmenting the VLANs and handling WAN traffic, should be provided by EANV. Changes in firewall rules will be governed by a change management process.	10
E14	2. High	E1.Cyber Security	Work stations should have an automatic, configurable time-out function to ensure an agent is automatically logged out after a configurable timeout.	10
E15	2. High	E1.Cyber Security	The solution should be integrated with the SIEM platform of EANV. At least syslog and security logs should be integrated.	10
E16	2. High	E1.Cyber Security	All components of the solution should be hardened with a minimum score of 80% according to the CIS benchmark.	10
E17	2. High	E1.Cyber Security	Permanent remote access should be done via an IPSec site-to-site VPN tunnel.	10
E18	2. High	E1.Cyber Security	The Participant should hold a valid ISO/IEC 27001 certification for an information security management system. The certification should be issued by an accredited certification body and should cover the organisational scope relevant to the development, implementation, maintenance and support of the offered CUPPS solution.	10
E19	2. High	E1.Cyber Security	The Participant should have a recent SOC 2 Type II report, or equivalent independent third-party assurance report, covering information security controls relevant to the development, implementation, maintenance and support of the offered CUPPS solution. The report should cover, as a minimum, security, availability and confidentiality controls and should relate to an audit period ending no more than twelve months before the Tender submission deadline. The Participant should provide the report, or an executive summary thereof, as part of its Tender.	10
E20	5. Question	E1.Cyber Security	Please describe how you continuously ensure that the solution has appropriate security levels and in accordance to standards.	N/A
E21	5. Question	E1.Cyber Security	Describe how identity management and user security is managed in the proposed solution and how security differs depending on the user role.	N/A
E22	5. Question	E1.Cyber Security	Describe how you manage authorizations for employees for accessing the solution at EIN through the site-to-site VPN tunnel.	N/A
E23	5. Question	E1.Cyber Security	If the Participant holds a valid ISO27001 certification, explain the scope of this certification.	N/A
E24	5. Question	E1.Cyber Security	If the Participant holds a valid SOC 2 report, explain the scope of this report.	N/A
E25	5. Question	E1.Cyber Security	Explain what cyber security breaches or significant incidents have happened within the scope of your (product) offering in the past 3 calendar years.	N/A
				480