Innovation of Diffractive Optically Variable Image Device for Electronic ID Cards (eID card) (reissue)

SECURITY AUDIT
for Production of DOVID design and MasterHologram

ANNEX 7 to the Agreement for supply of security elements for Czech electronic ID cards
No. 029/OS/2021(hereinafter referred to only as “Agreement”)

(hereinafter referred to as "this document")

1. Determination of subject matter

This document is relevant and describes conditions and requirements of all security audits defined by the Agreement, i.e.:

a) the initial Security Audit, i.e. an audit before signing the Agreement with the selected Contractor within the tender procedure;

b) all subsequent regular Security Audits and extraordinary Security audits carried out after the signing of the Agreement.

2. Determination of Parties

For the purposes of this document, the general designations of the Contracting Parties are used, where STÁTNÍ TISKÁRNA CENIN, státní podnik, Business ID: 0001279 is designated as the Contracting authority, and the Contractor as any entity, which shall be providing the performance of the subject matter of the Agreement (i.e. including also the preparation or production of the MasterHologram or any product that is the carrier of the DOVID design) as subcontractor/s of the Contractor and the Contractor remains responsible for fulfilment of these obligations and the Contractor is required toto assure cooperation on the subcontractor/s side.

3. Participation / personnel composition

The Security Audit will be performed by representatives of the Contracting authority (usually 1-2 persons) and facultatively with a support of representatives of an independent auditor who is a person accredited by the Czech Accreditation Institute, o.p.s. (where “o.p.s” stands for a “Community interest society” a form or a legal entity

recognised by the Czech law) or another authority according to the legal order of the given country.

If the Contractor raises any reservations to the course, manner of execution or outcome of the Security Audit, that was performed only by the Contracting authority, another Security Audit by an independent auditor as defined in the previous paragraph shall be subsequently arranged and performed.

For the Contractor is required to participate officer responsible for security, i.e. Security manager or an authorized person. Other persons may participate at the discretion of the Contractor.

4. Method of conducting the security audit:

The Security Audit will be performed in accordance with ISO 19011: 2019. The Security Audit will be carried out either physically on site or, if the current situation does not allow it, it will be carried out remotely (i.e. by videoconference in combination with a shared document depository) (hereinafter referred to as "**remote audit**").

5. Time course:

The Security Audit will usually be organized in two days with the following agenda:

• Day 1 - security policy, security documentation, risk management, business continuity management, ensuring security processes, building inspection,

• Day 2 - completion of the inspection of the building and inspection of the settings of security processes, processing of the minutes of the security audit, conclusion.

The remote audit agenda can be adjusted in terms of time schedule.

6. Date of the Security Audit:

The Contractor's contact person stated within the tender procedure will be informed of the Security Audit at least 5 days in advance in the case of an initial Security Audit, i.e. an audit before signing the Agreement with the selected Contractor within the tender procedure, and at least 30 days in advance in subsequent Security Audits, i.e. audits carried out after the signing of the Agreement.

7. Minimum requirements to be subject to Security Audit:

All information, terms and requirements in this document must be interpreted in the context of the relevant standards and general security principles (especially according to international standards series 27000 and the interpretation of the Czech National Cyber and Information Security Agency), system management (according to international

management system standards) and procedural procedures (according to the general principles of the procedural approach).

The Contractor must ensure compliance with all of the following requirements, all of which are based on the requirements in particular ISO 14298 and CWA 15374, and must be interpreted in accordance with ISO 14298 and CWA 15 374.

A fundamental document for assessing the fulfilment of the following requirements is the risk analysis prepared by the Contractor (see requirement 01 below), on which the method of meeting the individual requirements based on ISO 14298 and CWA 15374 is based:

No	Requirement	Further description on manner of fulfilling the requirement
01	A risk assessment and risk management document must be prepared and regularly updated	**Minimum level to fulfil the requirement**: The Contractor is obliged to have a risk analysis prepared and regularly updated (at least once a year), including the determination of the management of these risks to the extent of at least the ISO 14298 standard - point 4.4. The document must meet: (1) Requirements according to ISO 27001, or (2) must contain at least the following parts: • risk identification • risk analysis • risk evaluation • risk mitigation • risk management (resp. its mitigation) • risk monitoring and review **Manner of fulfilling in case of physical audit**: Submission of specific written documentation containing a risk analysis, including the management of these risks, which demonstrates compliance with the above minimum requirements. **Manner of fulfilling in case of remote audit**: Submission of specific written documentation containing a risk analysis, including the management of these risks, which demonstrates compliance with the above minimum requirements in the form of remote access or display on a shared screen.
02	A system of regular safety inspections of the Contractor's	**Minimum level to fulfil the requirement**:

No	Requirement	Further description on manner of fulfilling the requirement
	subcontractors, who supply him with input safety material for the production and finalization of products, must be set up and implemented	The Contractor is obliged to have set up and implemented a system of regular (at least once in a period of 3 years) security inspections of its subcontractors, who supply it with input security material for the production and finalization of products. For the purposes of this security audit, any control of a subcontractor that verifies compliance with the requirements of min. in the scope of points 1-12 according to this document shall be considered as the security inspection, while the form of such an inspection must be a security audit in personal / physical or remote form, or verification of the holding of ISO 14298 or CWA 15 374 certificates. The scope and manner of performing these security inspections may differ from the above stated minimal requirements if this different procedure is in accordance with the Contractor's risk analysis (i.e. the document according to requirement 01 in this document). **Manner of fulfilling in case of physical audit**: Submission of specific written documentation containing the settings of the above required system of security inspections (i.e. especially the internal documentation of the Contractor), including documentation of min. 1 sample in the sense of proving the performance of a specific security inspection of the subcontractor meeting the above requirements in the last min. 3 years from the date of the ongoing Security Audit. **Manner of fulfilling in case of remote audit**: Submission of specific written documentation containing the settings of the above required system of security inspections (i.e. especially the internal documentation of the Contractor), including documentation of min. 1 sample in the sense of proving the performance of a specific security inspection of the subcontractor meeting the above requirements in the last min. 3 years from the date of the ongoing security audit in the form of remote access or display on a shared screen.

No	Requirement	Further description on manner of fulfilling the requirement
03	A system of concluding confidentiality agreements with the Contractor's subcontractors must be set up and implemented	**Minimum level to fulfil the requirement**: The Contractor is obliged to have set up and implemented a system of concluding confidentiality agreements with its subcontractors, which contain at least the following parts: • Names of parties to the agreement, • Definition of what constitutes confidential information, • Prohibiting any exclusion from confidentiality (except for legal and other generally binding obligations to publication of information) • Relevant time period, • Fines and sanctions in the appropriate amount according to the risk analysis The specific mandatory requirements and the final form of these confidentiality agreements may differ from the above stated minimal requirements if this different procedure is in line with the Contractor's risk analysis (i.e. the requirement 01 document in this document). **Manner of fulfilling in case of physical audit**: Submission of specific written documentation containing the settings of the required system (i.e. especially the internal documentation of the Contractor), including documentation of min. 1 sample in the sense of proving the conclusion of a specific agreement on confidentiality with a subcontractor meeting the above requirements. **Manner of fulfilling in case of remote audit**: Submission of specific written documentation containing the settings of the required system (i.e. especially the internal documentation of the Contractor), including documentation of min. 1 sample in the sense of proving the conclusion of a specific confidentiality agreement with the subcontractor meeting the above requirements in the form of remote access or display on a shared screen.
04	Security procedures must be set up and implemented	**Minimum level to fulfil the requirement**: The Contractor is obliged to have prepared and implemented security procedures and rules for the production and delivery of safety products. The whole process must be described, from the purchase of raw

No	Requirement	Further description on manner of fulfilling the requirement
		materials / semi-finished products, the production cycle to the dispatch and transport of the products to the customer. The documentation must include a record of materials during the production cycle, i.e. ensuring that the Contractor knows (knows / is known to the Contractor) at all times (at each production step) where and how much material is located, while the same process must be set after production step, and the same procedure must be set in case disposal of non-conforming production. The rule of traceability must be observed - the ability to trace the history, use or location of what is being assessed. The scope and manner of fulfilling of these requirements may differ from the above stated minimal requirements if this different procedure is in line with the Contractor's risk analysis (i.e. the requirement 01 document in this document). **Manner of fulfilling in case of physical audit**: Submission of specific written documentation containing the above required security processes and rules (i.e. especially the Contractor's internal documentation), including documentation of min. 1 sample in the sense of proving the implementation of the given processes and rules meeting the given documentation. **Manner of fulfilling in case of remote audit**: Submission of specific written documentation containing the above required security processes and rules (i.e. especially the Contractor's internal documentation), including documentation of min. 1 sample in the sense of proving the implementation of the given processes and rules meeting the given documentation in the form of remote access or display on a shared screen.
05	A system of regular internal Security Audits must be set up and implemented	**Minimum level to fulfil the requirement**: The Contractor is obliged to have set up a system of regular (at least once a year) internal security audits of its own procedures and rules in the scope of at least according to the ISO 14298 standard - point 9.2. Performing the security audits may be part of internal audits.

No	Requirement	Further description on manner of fulfilling the requirement
		<u>Manner of fulfilling in case of physical audit</u>: Submission of specific written documentation containing the settings of the above required system of internal security audits (i.e. especially the internal documentation of the Contractor), including documentation of min. 1 sample in the sense of proving the performance of a specific internal security audit meeting the above requirements in the last year from the date of the ongoing Security Audit. The Contractor is also obliged to document the record of such an audit and information on the implementation of corrective measures in case of identified deficiencies, if relevant, and the current program / plan of internal audits, if it is prepared. **<u>Manner of fulfilling in case of remote audit</u>**: In the form of remote access, or display on a shared screen, the submission of specific written documentation containing the settings of the required system of internal security audits (i.e. especially the internal documentation of the Contractor), including documentation of min. 1 sample in the sense of proving the performance of a specific internal security audit meeting the above requirements in the last year from the date of the ongoing security audit. The Contractor is also obliged to document the record of such an audit and information on the implementation of corrective measures in case of identified deficiencies, if relevant, and the current program / plan of internal audits, if it is prepared.
06	The so-called Business Continuity Plan of the Contractor must be prepared	**<u>Minimum level to fulfil the requirement</u>**: The Contractor is obliged to have prepared a so-called Business Continuity Plan of the Contractor in order to ensure the uninterrupted supply of products or services and to ensure maximum protection in order to ensure the operation of the company and its operation in situations where the company is threatened or facing a disaster, and this document must meet the following minimum requirements: (1) the requirements of the standard according to ISO 22301, or

No	Requirement	Further description on manner of fulfilling the requirement
		(2) must contain at least the following parts: • Risk and threat analysis • Business impact analysis • Crisis measures and organizational guidelines to keep the organization in crisis • Plans and measures to maintain continuity • Scenarios, plans and measures for recovery of operation • Techniques for quality assurance, preventive measures such as maintenance, exercises, audits • Contact information for members of management (especially crisis) • Instructions for employees in the event of a crisis • Allocation of people, tools, and other resources The scope and manner of fulfilling of these requirements may differ from the above stated minimal requirements if this different procedure is in line with the Contractor's risk analysis (i.e. the requirement 01 document in this document). **Manner of fulfilling in case of physical audit**: Submission of specific documentation demonstrating compliance with the above minimum requirements. **Manner of fulfilling in case of remote audit**: Submission of specific documentation that demonstrates compliance with the above minimum requirements in the form of remote access or display on a shared screen.
07	The Contractor's production and storage facilities must be secured by the following systems: IDS (Intrusion Detection System), FS (Fire System), CCTV, ACS (Access Control System)	**Minimum level to fulfil the requirement**: The Contractor is obliged to provide and equip the Contractor's production and storage facilities with defined security systems (IDS, FS, CCTV, ACS) with connection to the monitoring center (internal or external), while the following minimum requirements must be met: - CCTV must be recorded and must monitor the entire production area and perimeter without blind spots. - ACS must be installed at least at all entrances to the production premises.

No	Requirement	Further description on manner of fulfilling the requirement
		- IDS must fully cover at least all production premises, production preparation and storaget premises. - FS is not mandatory if this fact is stated in the "Fire safety solution" or a similar document. The scope and manner of fulfilling of these requirements may differ from the above stated minimal requirements may differ from the above if this different procedure is in line with the Contractor's risk analysis (i.e. the requirement 01 document in this document). **Manner of fulfilling in case of physical audit**: Physical inspection of the installed security technology, visit to the monitoring center, submission of the document "Description of physical and logical perimeter," or "Security project" or the directive "Physical protection" or similar documents describing the installed security technologies, including "Fire safety solution" or a similar document, if relevant, and proving compliance with the above minimum requirements. **Manner of fulfilling in case of remote audit**: Submission of specific documents "Description of the physical and logical perimeter, or "Security project" or the directive "Physical Protection" or similar documents describing the installed security technologies demonstrating compliance with the above minimum requirements, including "Fire safety solution" or a similar document, if relevant, remote access or shared screen display the documentation must be photographs of the installed technologies, or document the security features installed by the camera as part of the online transmission, which will document compliance with the minimum requirements).
08	Space must be designated for loading and unloading goods and materials	**Minimum level to fulfil the requirement**: The Contractor is obliged to have a marked area for loading or unloading goods and material and this area must be operated in security mode (i.e. min. PZTS, ACS and CCTV with a record that monitors the entire area without blind spots). At the time of loading / unloading, only

No	Requirement	Further description on manner of fulfilling the requirement
		the operator handling the goods or materials and, if necessary, guarding must be present in the area. The scope and manner of fulfilling of these requirements may differ from the above stated minimal requirements may differ from the above if this different procedure is in line with the Contractor's risk analysis (i.e. the requirement 01 document in this document). **Manner of fulfilling in case of physical audit**: Physical inspection of the space, submission of the document "Description of physical and logical perimeter, or" Security project "or the directive" Physical protection "or similar documents describing the security of loading / unloading areas that demonstrate compliance with the above minimum requirements, the documentation must include photographs of the installed technologies that will document compliance with the minimum requirements. **Manner of fulfilling in case of remote audit**: Submission of documents "Description of the physical and logical perimeter, or" Security project "or the" Physical Protection "Directive or similar documents describing the security of loading / unloading areas demonstrating compliance with the above minimum requirements, by remote access or display on a shared screen (the documentation must include photographs of the installed technologies, that will document compliance with the minimum requirements).
09	Physical security must be performed by the Contractor's own staff or by an external qualified entity	**Minimum level to fulfil the requirement**: The Contractor is obliged to ensure continuous physical security of its facilities by its own employees or by an external qualified entity that is authorized to perform the physical security in accordance with the law. All production and storage facilities of the Contractor related to the performance of the public contract must be secured against the intrusion and entry of unauthorized persons, detailed inspection of the interior from the outside or the presence of unauthorized persons. E.g. it must have adequate perimeter security (fencing) and mechanical security of all entrances (grilles on windows, hardened entrances-doors, etc.)

No	Requirement	Further description on manner of fulfilling the requirement
		The scope and manner of fulfilling of these requirements may differ from the above stated minimal requirements may differ from the above if this different procedure is in line with the Contractor's risk analysis (i.e. the requirement 01 document in this document). **Manner of fulfilling in case of physical audit**: Physical inspection of the security area and mechanical security systems, submission of a document "Description of physical and logical perimeter", or document "Security project" or directive "Physical protection" or similar documents describing the state of physical security, which demonstrates compliance with the above minimum requirements. The Contractor must submit photographs of the security of the building, which will document the fulfilment of the minimum requirements, and in the case of an external entity, the Contractor must document the concluded valid contract on ensuring physical security between the Contractor and the external entity. **Manner of fulfilling in case of remote audit**: Submission of a document "Description of the physical and logical perimeter, or a document" Security project "or a directive" Physical protection "or similar documents describing the state of physical security demonstrating compliance with the above minimum requirements, by remote access or display on a shared screen. The Contractor must submit photographs of the security of the building, which will document the fulfilment of the minimum requirements, and in the case of an external entity, the Contractor must document the concluded valid contract on ensuring physical security between the Contractor and the external entity.
10	A key management must be implemented	**Minimum level to fulfil the requirement**: The Contractor is obliged to have a transparent key regime implemented, which ensures the registration, allocation, and secure storage of keys. The key mode system must be inspected at least once a year.

No	Requirement	Further description on manner of fulfilling the requirement
		The scope and manner of fulfilling of these requirements may differ from the above stated minimal requirements may differ from the above if this different procedure is in line with the Contractor's risk analysis (i.e. the requirement 01 document in this document). **Manner of fulfilling in case of physical audit**: Physical inspection of the registration system and key storage, documentation of specific documentation that the inspection of the key regime system is performed at least once a year, i.e. the Contractor must submit at least a record of the inspection in the last year from the date of the ongoing security audit. **Manner of fulfilling in case of remote audit**: In the form of remote access or display on a shared screen, the Contractor must document documents from which it is clear that the key mode is implemented (photo documentation of key storage must be included) and document specific documentation that the records of assigned keys are checked at least once a year, i.e. the Contractor must provide at least a record of the inspection in the last year from the date of the ongoing security audit.
11	They must be processed and implemented the principle of access to information systems during and upon termination of employment	**Minimum level to fulfil the requirement**: The Contractor is obliged to have developed and implemented the principles of controlled access to information systems during and upon termination of employment of the Contractor's employees. **Manner of fulfilling in case of physical audit**: Submission of specific written documentation containing the setting of the above required principles (i.e. especially the internal documentation of the Contractor, e.g. output sheet), including documentation of min. 1 sample in the sense of proving the implementation of the given principles meeting the above requirements. **Manner of fulfilling in case of remote audit**: Submission of specific written documentation containing the setting of the above required principles (i.e. especially the internal documentation of the Contractor, e.g. output

No	Requirement	Further description on manner of fulfilling the requirement
		sheet), including documentation of min. 1 sample in the sense of proving the implementation of the given principles meeting the above requirements in the form of remote access or display on a shared screen.
12	The Contractor has its own employees to ensure the production and storage of security products, or agency employees who meet other conditions	**Minimum level to fulfil the requirement**: The Contractor is obliged to ensure the production and storage of security products by its own employees or by an agency staff. If they use agency staff, they must have a signed confidentiality agreement (to the minimum extent of point 03 of this document), both with their own staffing agency and with the Contractor. At the same time, there must be a confidentiality agreement (to the minimum extent of point 03 of this document) between the Contractor and the recruitment agency. For the purposes of this security audit, Agency Employment is the temporary placement of an employment agency employee to perform work for an employer on the basis of an employment contract or also in the form of an employment agreement concluded between the employee and the employment agency. In this case, the user does not "take" temporarily placed employees from the agency, but only "hires" them for a period of time. At the same time, agencies may not demand payment from agency staff - the user pays the agency. **Manner of fulfilling in case of physical audit**: Submission of specific written documentation proving compliance with the requirement (i.e. especially personnel records). **Manner of fulfilling in case of remote audit**: Submission of specific written documentation proving the fulfilment of the given requirement (i.e. especially personnel records) in the form of remote access or display on a shared screen.