Acquisition Directorate
peter.kowalski@ncia.nato.int

NCIA/ACQ/2022/07012
26 August 2022

Market Survey - Request for Information

Identity and Access Card Management System

NCI Agency Reference: MS-CO-115678-IAMS

The NCI Agency is seeking information from Nations and their qualified Industry in order to assess the feasibility of the delivery of a Commercial-Off-The-Shelf (COTS) Identity and Access Card Management System.

NCI Agency Point of Contact
Senior Contracting Officer: Peter Kowalski
E-mail: Peter.Kowalski@ncia.nato.int **and** Maria.Huerga@ncia.nato.int

To: See Distribution List

Subject: NCI Agency Market Survey
Request for information MS-CO-115678-IAMS

1. NCI Agency requests the assistance of the Nations and their Industry to identify currently available Commercial-Off-The-Shelf (COTS) solutions to meet the requirements for an identity and access card management system.

2. This Market Survey is being issued to identify potential solutions and possible suppliers.

3. The broadest possible dissemination by Nations of this Market Survey Request to their qualified and interested industrial base is requested.

4. Responses shall in all cases include the name of the firm, telephone number, e-mail address, designated Point of Contact, and a NATO UNCLASSIFIED description of the capability available and its functionalities. This shall include any restrictions (e.g. export controls) for direct procurement of the various capabilities by NCI Agency.

5. The NCI Agency reference for this Market Survey Request is MS-CO-115678-IAMS, and all correspondence and submissions concerning this matter should reference this number.

6. A summary of this emerging requirement is set forth in the ANNEX B attached hereto.

7. Other supporting information and documentation (technical data sheets, marketing brochures, catalogue price lists, descriptions of existing installations, etc..) are also desired.

8. Market Survey responses will be assessed against the input received from the questions in ANNEX C – Market Survey Questionnaire. Annexes B and D provide details of the desired technical requirements.

9. Responses are due back to NCI Agency no later than **17:00 hours Brussels time on 24 October 2022**.

10. Please send all responses, via email, using MS-CO-115678-IAMS in the title of the email to: Peter.Kowalski@ncia.nato.int **and** Maria.Huerga@ncia.nato.int.

11. The NCI Agency reserves the right to request a solution demonstration of the described solution. However, given the current global landscape, any solution demonstration will likely be delivered via video conferencing tool at the discretion of the Market Survey Respondent. Respondents are advised to await further instructions after their submissions and are requested not to contact any NCI Agency staff directly other than the POC identified above in Paragraph 10.

12. Any response to this request shall be provided on a cost-free and voluntary basis. Responses to this request, and any information provided within the context of this survey, including but not limited to pricing, quantities, capabilities, functionalities and requirements will be considered as indicative and informational only and will not be considered as binding on the participant or on NATO within the context of any future acquisition.

13. The NCI Agency is not liable for any expenses incurred by firms in conjunction with their participation in this Market Survey and this Survey shall not be regarded as a commitment of any kind concerning future procurement of the items described.

14. Your assistance in this Market Survey request is greatly appreciated.

For the Chief of Acquisition

[*Original Signed By*]

Peter Kowalski
Senior Contracting Officer

Enclosures:

1. ANNEX A - Distribution List
2. ANNEX B - Market Survey Requirements
3. ANNEX C - Market Survey Questionnaire
4. ANNEX D - EBS System and User Requirements

ANNEX A.

Distribution List for Market Survey

Potential Industrial Suppliers (including NCI Agency BOA Holders)

NATO Delegations (Attn: Military Budget Committee or Infrastructure Adviser):

Albania	1
Belgium	1
Bulgaria	1
Canada	1
Croatia	1
Czech Republic	1
Denmark	1
Estonia	1
France	1
Germany	1
Greece	1
Hungary	1
Iceland	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
Montenegro	1
The Netherlands	1
North Macedonia	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Türkiye	1
United Kingdom	1
United States	1

Belgian Ministry of Economic Affairs 1

Embassies in Brussels (Attn: Commercial Attaché):

Albania	1
Bulgaria	1
Canada	1
Croatia	1
Czech Republic	1
Denmark	1
Estonia	1

France	1
Germany	1
Greece	1
Hungary	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
Montenegro	1
The Netherlands	1
North Macedonia	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Türkiye	1
United Kingdom	1
United States (electronic copy to brussels.office.box@mail.doc.gov)	1

Distribution for information

NATO HQ

NATO Office of Resources	
Management and Implementation Branch – Attn: Deputy Branch Chief	1
NATO HQ C3 Staff	
Attn: Executive Co-ordinator	1

NCI Agency – Internal Distribution

ACQ Chief of Acquisition	1
ACQ Deputy Chief of Acquisition	1
ACQ Principal Contracting Officer	1
ACQ Principal Contracting Assistant	1
SSBA Service Line Chief	1
EBA Program Manager	1
SSBA Service Area Owner	1
SSBA Service Delivery Manager	1

NCI Agency – NATEX

All NATEX	1

Industrial distribution

COUNTRY	VENDOR
ALBANIA	
	TCN shpk
BELGIUM	
	ATOS
	BARCO N.V. / BARCO Control Rooms
	BATS (Belgian Advanced Technology Systems) S.A.
	Brevco Services S.C.S.
	Computer Sciences Corporation (CSC)
	Concurrent Technologies Corportation (CTC)
	Deloitte Consulting and Advisory Bv
	Devoteam NV/SA
	Dimension Data Belgium
	Ericsson NV/SA
	Gartner Belgium B.V.B.A
	Getronics Belgium S.A.
	Gravitence BVBA
	IBM Belgium BV/SRL
	IDtech S.A.
	NCTS SPRL
	PricewaterhouseCoopers Enterprise Advisory BV/SRL
	RHEA System S.A.
	Siemens
	Sogeti Belgium NV/SA
	Sopra Steria Benelux S.A.
	System Solutions Belgium NV
	Telespazio Belgium Srl (former Vitrociset Belgium)
	Thales S.A.
	Unify Communications NV
	Unisys Belgium S.A.
BULGARIA	
	Electron Progress EAD
	Kristanea Ltd.
	Lirex BG Ltd.
	SmartCom-Bulgaria AD
	TechnoLogica EAD
CANADA	
	Compusult Ltd.
	Entrust Ltd.
	General Dynamics Mission Systems-Canada
	MDA Ltd. (formerly MacDonald, Dettwiler and Associates Ltd.)
	Resul Control Systems Ltd.

	RHEA Inc.
	Sabytel Technologies Inc.
	Tangiers Canada Ltd.
	Valcom Consulting Group Inc.
CROATIA	
	B4B Ltd.
	CROZ d.o.o. za informaticku djelatnost
	KING ICT d.o.o
	Senso IS d.o.o.
	Span PLC
CZECH REPUBLIC	
	Autocont a.s.
	Damovo Česká republika s.r.o.
	GTS Czech, s.r.o.
	Techniserv, s.r.o.
	TietoEnator Czech s.r.o.
DENMARK	
	Danoffice IT ApS
	Dencrypt A/S
	Ebicon ApS
	Entrust Datacard Denmark A/S (Includes SMS Passcode)
	Ifad Ts A/S
	Saab Danmark A/S
	Systematic A/S
	Terma A/S
ESTONIA	
	Aktors OÜ
	Telegrupp AS
FRANCE	
	Airbus Defence and Space SAS
	Alsid SAS
	Alter Défense
	Altran Technologies SA (ASD)
	APPI Technology SAS
	Astrium SAS
	ATDI SA (Advanced Topographic Development & Images)
	Bull SAS
	Capgemini Consulting SAS
	CS Systèmes d'Informations SAS
	Naval Group (ex DCNS)
	Evolis SAS
	Global Technologies SAS
	Khiplus Advance
	LGM Group SAS
	Sopra Steria Group

	Thales SIX GTS France SAS
	THALES DIS FRANCE SA
GERMANY	
	]init[AG für Digitale Kommunikation
	Aditerna GmbH
	Airbus Defence and Space GmbH (ex EADS GmbH)
	Atos Origin GmbH
	Bechtle GmbH & Co.KG
	Carl-Otto Schartenberg GmbH
	CGI Germany GmbH & Co KG
	CONET Solutions GmbH
	Cordsen Engineering GmbH
	CSC Deutschland Solutions GmbH
	ESG Elektroniksystem - und Logistik GmbH
	Frequentis Deutschland GmbH
	Hays AG
	HID Global Corporation
	IABG mbH
	INTEC Industrie-Technik GmbH & Co. KG
	KB Impuls Service GmbH
	LOG GmbH
	Materna GmbH
	Nexus-Group GmbH
	NSSL Global GmbH
	PCS Systemtechnik GmbH
	Rohde & Schwarz GmbH & Co. KG.
	Telespazio Germany GmbH
	Thales Deutschland GmbH
	T-Systems International GmbH
	Vega Deutschland GmbH & Co. KG
GREECE	
	Altec Integration S.A.
	Cosmos Business Systems S.A.
	European Dynamics S.A.
	ISI Hellas S.A.
	Onex S.A.
HUNGARY	
	Siemens PSE Kft.
	Synergon Information Systems Plc. - Synergon Informatika Rt.
ICELAND	
	Advania hf.
ITALY	
	3F & EDIN S.p.A.
	CapGemini Italia S.p.A.
	D'Appolonia S.p.A.

	Elesia – Elettronica e Sistemi per Automazione S.p.A.
	Elex S.r.l.
	Engineering Ingegneria Informatica S.p.A
	IES S.r.l.
	Intecs S.p.A.
	Itel Srl
	Leonardo Electronics Division
	Netgroup S.r.l.
	Simav S.p.A
	SMS Engineering S.r.l.
	Telsy S.p.A.
	Vitrociset S.p.A.
LATVIA	
	Baltic Information & Security Systems
	Datakom Ltd
	DATI Group, LLC
	DPA Ltd
	SIA Fima
LITHUANIA	
	Automatikos sistemos UAB
	Ingenious IT UAB
	iTree Lietuva UAB
	Novian Technologies UAB
	UAB NRD CS
LUXEMBOURG	
	LuxTrust S.A.
	NTT Luxembourg PSF S.A.
	PWC - PricewaterhouseCoopers Société coopérative
NETHERLANDS	
	Alten Nederland B.V.
	Capgemini Nederland B.V.
	Castor Networks B.V.
	ComActivity Benelux B.V.
	Crosscheck Networks Nederland B.V
	Delft Dynamics B.V.
	iDelft B.V.
	Intergraph Benelux B.V.
	Nsecure B.V.
	NCIM Groep B.V.
	Rohde & Schwarz Benelux B.V
	Sioux Automation Technology B.V
	SMT Simple Management Technologies B.V.
	SYSQA B.V.
	TNO Defence, Safety, and Security

NORWAY	
	3D perception AS
	Atea Norge AS
	Kongsberg Defence & Aerospace AS (KDA)
	MaXware AS
	Teleplan AS
POLAND	
	Asseco Poland S.A.
	Atende S.A.(prior ATM S.A.)
	Comarch S.A.
	Enamor Sp. z.o.o
	Exence S.A.
	Hertz Systems Ltd Sp. z o.o.
	KenBIT Sp. z o.o.
	MGR Integration Solutions Polska
	Newind sp. z o.o.
	Ośrodek Badawczo-Rozwojowy Centrum Techniki Morskiej S.A.
	Unizeto Technologies SA
	Vector Synergy Sp. z o.o.
	VOL Sp. z o.o. Sp.k.
	Wasko S.A.
	XComp Sp. z o.o.
	Zbar Phu Mariusz Popenda
PORTUGAL	
	Deimos Engenharia S.A.
	GMV- Skysoft S.A.
	Indra Sistemas Portugal S.A.
ROMANIA	
	ATOS Convergence Creators Srl
	Certsign S.A.
	Interactive Software Srl
	Kranszwald Srl
	Marctel S.I.T. Srl
	REXENERG POWER Srl
	Romsys Srl
	Teamnet International S.A.
	Technology Systems and Services International Srl
	UTI Grup S.A.
SLOVAKIA	
	Aliter Technologies a.s
	Unistar LC d.o.o.
SPAIN	
	ACT Sistemas SL
	Deloitte SL
	GMV Aerospace and Defence, S.A.U

Grupo SPEC, S.A.
Indra Sistemas S.A.
KRC Española, S.A.
Nextel Aerospace Defence and Security S.L. (NADS)
NTT DATA
Primion Digitek S.l.u.
Safelayer Secure Communications S.A.
SENER Ingenieria y Sistemas S.A.
Thales Programas Electrónica y Comunicaciones S.A.

T ÜRKIYE

Altay Kollektif Şirketi M. Murad Dural ve Ort.
Aselsan Elektronik San. ve Tic. A.Ş
Atos Bilişim ve Danışmanlık A.Ş.
C TECH Bilişim Tek. San Tic. A.Ş
Esen Sistem Entegrasyon ve Müh. Hiz. San ve Tic. Ltd. Şti.
Havelsan Hava Elektronik San. Ve Tic. A.Ş
ICterra Bilgi ve İletişim Teknolojileri San. ve Tic. A.Ş
Meteksan Savunma Sanayi A.Ş.
Obss Teknoloji A.Ş.
Simsoft Computer Technologies Ltd
STM Savunma Teknolojileri mühendislik ve Tic. A.Ş
Tubitak Bilgem Türkiye Bilimsel Ve Teknolojik Araştirma Kurumu Başkanlığı

UNITED KINGDOM

3SDL Ltd
Airbus Defence and Space Ltd (UK)
Audax Global Solutions Ltd.
BAE Systems Applied Intelligence Ltd.
BMT HI-Q Sigma Ltd.
C4i Systems Ltd.
Centerprise International Ltd.
DP Connect Ltd.
Entrust
General Dynamics United Kingdom Ltd.
ISG Information Services Group, Inc.
Leonardo MW LTDSelex ES Ltd.
Leonardo UK Ltd.
Lockheed Martin UK INSYS Ltd.
Northrop Grumman Mission Systems Europe Ltd.
Remsdaq Ltd.
Savi Technology UK Ltd.
Sopra Steria Ltd.
Total IA Ltd.
Tricis Ltd.
TrustID Ltd.
Universal Defence and Security Solutions Ltd (UDSS)

UNITED STATES

Advantidge, Inc. - Identity Management Solutions
Affigent, LLC
Alion Science and Technology Corp.
Applied Coherent Technology Corp.
BAE Systems Information Solutions, Inc.
Booz Allen & Hamilton, Inc.
CACI Inc. - Federal
Creative Information Technology, Inc.
Computer Sciences Corporation (CSC) North American Public Sector
Daon, Inc.
DataPath, Inc.
Decypher Technologies, Ltd.
EDO Corporation
Elliott Data Systems, Inc.
EMW, Inc.
G2, Inc.
General Dynamics Information Technology, Inc. (GEDIT)
Guident Technologies, Inc.
Honeywell Technology Solutions, Inc.
Houston Associates
Hyperion, Inc.
Kymeta Corp.
Legend ID
Leidos, Inc.
Level 3 Communications, LLC
LMI - Logistics Management Institute
Lockheed Martin Corp.
Ma Federal, Inc. (DBA Igov.com)
MCR Federal, Inc. (USA)
Northrop Grumman Information Technology, Inc.
Ntt Data Services Federal Government, LLC
Parsons Government Services, Inc.
PlanIT Group, LLC
Ravenswood Solutions, Inc.
Raytheon Company Network Centric Systems (NCS)
SAIC, Inc.
Tbw Global, LLC
Teledyne Brown Engineering, Inc.
Telos Corp.
The Boeing Company
The RAND Corp.
Unisys Corp.

ANNEX B.

MARKET SURVEY REQUIREMENTS FOR IDENTITY AND ACCESS CARD MANAGEMENT SYSTEM

1. Scope

1.1. The NCI Agency is performing a market survey in order to identify currently available and non-developmental identity and access cards management systems/solutions on the market which fulfil the requirements presented below. At this stage, NCI Agency is seeking to evaluate all the available systems/solutions on the market which can provide technological, robust, capable and cost effective solution to NATO.

1.2. The system shall be capable of being deployed and used within NATO, NATO Nations and during NATO deployed operations, and only those software solutions which have intellectual property rights fully residing in NATO member countries will be considered.

2. Current NCI Agency Identity and Access Management Solution

2.1. The Agency is currently using an identity and access card management system based on COTS software customized to meet Agency needs.

2.2. The workflows and forms used to capture and present data within the current platform cover a wide range of both size and complexity. Current system provides integration options (receiving and sending data) with 3rd party systems via web services, custom SQL tables/databases and custom protocol integration.

2.3. Current system supports PKI and PIV2, replication of data between multiple instances.

2.4. The current platform is deployed operationally on a single network as well as in a development environment in Microsoft Azure. In production there is a need of distributing the load to the application servers by utilizing a load balancer and high availability databases. Currently the architecture is a client-server architecture with the dedicated clients, application server, web application and integration with other systems.

3. Desired Requirements/Functionalities

3.1 The goal of this Survey is to identify and evaluate suitable COTS Identity and Access Card Management Systems which already include the acquisition and management of personnel biometrics (minimum photographs and signatures), and which could issue identity cards for the use of the NCI Agency and other NATO entities.

3.2 Please refer to Annex D of this Market Survey and note the defined “Must Have” requirements.

4. Life Cycle information

4.1 The solution/system design should minimise total system life cycle costs, including its future Operations and Maintenance (O&M, consumables, etc...).

4.2 The software and hardware environments within NATO are currently in the process of being upgraded by the IT Modernisation project based on a modern data centre approach. However, note that the majority of the NATO systems run on Microsoft/LINUX operating systems and must be capable of running in a virtual environment (VMWare Hypervisor).

ANNEX C.

1. Questionnaire

Company Name and Address:

Contact Name & Details:

Notes:

1. Please **DO NOT** alter the formatting. If you need additional space to complete your text then please use the 'Continuation Sheet' at the end of this Annex and reference the question to which the text relates to.

2. Please feel free to make assumptions, ***HOWEVER*** you must list your assumptions in the spaces provided.

3. Please **DO NOT** enter any company marketing or sales material as part of your answers within this market survey. But please submit such material as enclosures with the appropriate references within your replies. If you need additional space, please use a continuation sheet and clearly refer to the question being answered

4. Please **DO** try and answer the relevant questions as comprehensively as possible.

5. All questions within this document should be answered in conjunction with the summary of requirements in ANNEX B.

6. All questions apply to Commercial responders as appropriate to their Commercial off the Shelf (COTS) non-developmental products.

7. Cost details required in the questions refer to indicative Rough Order of Magnitude (ROM) estimates and shall include all assumptions the indicative estimate is based upon.

2. General Questions

1. Do you have an in-service Identity and Access Card Management System platform that currently meets the requirements as detailed in ANNEX B.

2. With the goal to understand the level of maturity and sustainability of your proposed solution, please address in detail the following points:

    - **a**) how long your proposed solution has been on the COTS market
    - **b**) what approximate market share has solution achieved in comparison with your peer competition
    - **c**) provide indications and evidence that your proposed solution is robust, non-developmental, and technologically and financially sustainable both in implementation and Operations and Maintenance.

3. Can your solution be entirely implemented and deployed on premise?

4. Provide details of where it is currently being used along with number of records it manages and the number of users.

5. What is the scope of the normally offered and required in-service support package?

6. What is scope and the duration training available for the various User roles?

3. Detailed Questions

1. COTS Solution

1.1. Please indicate the Requirement IDs in Annex D where your solution either does not or only partially fulfils.

1.2. Please briefly describe the technical implementation/deployment of your Identity and Access Card Management System and describe a typical system implementation within an organization similar to NATO?

1.3. Please describe a typical platform architecture and the typical technical requirements of your platform, including high availability and load balanced configurations.

1.4. Do you currently offer an on premise solution? Do you intend to continue to support said on premise solution for at least the mid-term future (3-5 years)?

1.5. What is the future timeline of planned feature enhancements for the near future (1-3 years)?

1.6. Please briefly describe how new workflows[1] are built using your platform and describe the level of flexibility and complexity supported, as well as describing any limitations on workflow flexibility and complexity.

1.7. Please describe the packaging and deployment process for workflows built using your platform.

1.8. Please describe the method/nature of your platforms integration with external data sources (Microsoft SQL Server, Oracle, PostgreSQL, Rest API, SOAP API, proprietary protocol, file export/import, ssh commands).

1.9. Please describe how integration with external data sources can be customized and how new integrations can be implemented.

1.10. Please describe how system security can be defined using your platform.

1.11. Please describe how your UI corresponding to workflow (web forms and client UI) is built.

1.12. Please describe the level of flexibility and complexity within the forms integrated with your BPA/Workflow platform.

1.13. Please describe how the forms are made available for the clients (dedicated or web).

[1] Workflow: succession of steps/states that defines the process of managing an identity

1.14. Please describe any out-of-the-box administrative features provided by your platform (workflow security, error log)

1.15. Please list standard/out of the box biometrics supported hardware.

1.16. Please list standard/out of the box card printing hardware.

1.17. Please confirm if the systems works with the following existing hardware:
- Toppan CP500 Card Printer,
- Datacard CD800 Card Printer,
- Nisca PR-C201 Printer,
- Topaz signature pad,
- Logitech web cameras,
- HID Omnikey RFID card reader,
- Honeywell barcode reader,
- LENEL access control system,

1.18. Please describe customisations available for captured input data.

1.19. Please describe to which extent and how the layout of badges can be customized.

1.20. Please provide us with any additional capabilities of your COTS solution that go above and beyond those included in ANNEX B.

1.21. Please list advantages & possible disadvantages of your product/solution/organization.

1.22. When migrating to your platform, do you provide tools to check data validity and identify records that could have problems?

1.23. Please describe the patch release process and feature adding process for clients and server software.

1.24. Please describe the personal data protection measures within the system and examples of data protection frameworks the system is currently in use/compliant with.

1.25. Any other supporting information you may deem necessary including any assumptions relied upon.

1.26. Please describe what standards are supported for your issued cards/tokens.

1.27. Please describe the cards used including durability and security features.

2. Rough Order of Magnitude (ROM) price data

2.1. Please provide ROM indicative pricing data for your Identity and Access Card Management System (application, licence(s) and required peripherals, consumables). You can assume pricing based on an unlimited number of

licenced entities (number of instances, number of users).

2.2. Please provide details and indicative pricing for the Annual O&M support package of the tool.

ANNEX D.
Identity and Access Card Management System Requirements

Requirements ID	Description	MoSCoW Priority
Identity and Access Card Management System – Server features		
IMS_TECH_01_01	On-Premise Platform implementation	Must
IMS_TECH_01_02	Stand-alone system	Must
IMS_TECH_01_03	System must provide integration options (receiving and sending data) with 3rd party systems via web services and custom SQL tables/databases	Must
IMS_TECH_01_04	Integration must be configurable from the point of view of fields correspondence;	Must
IMS_TECH_01_05	System must use HTTPS;	Must
IMS_TECH_01_06	System must support redundancy in active-active and active-passive configurations;	Must
IMS_TECH_01_07	System must support both load balancers/reverse proxies as web frontends and serving the requests by themselves;	Must
IMS_TECH_01_08	System must support NPKI (NATO PKI)[1], PKI and FIPS 201 PIV;	Must
IMS_TECH_01_09	System must support replication of data between multiple instances;	Must
IMS_TECH_01_10	System must support executing custom tasks periodically;	Must
IMS_TECH_01_11	System must be able to save all information needed to trace activities in an audit log;	Must
IMS_TECH_01_12	System must support exporting logs in a structured format for automated post-processing and analysis.	Must
Identity and Access Card Management System – Functional features		
IMS_TECH_02_01	**General information:** Server system must allow from the web browser: - the general system administration operations; - administration of items related to badge issuance, revocation, lifecycle management; - enrolment of personal information and biometrics; - reports generation; - access audit features. Server system must communicate also with dedicated clients running on dedicated workstations.	Must
IMS_TECH_02_02	**Authentication:** **User Name/Password or Single Sign On with ADFS claim authorization support for Web;** **User groups features:** Access must be allowed only to authenticated users. User accounts must: - identify an operator by a username and a password and have additional operator personal data; - be part of a group that grants them access to various system features; - be controlled by security policies (e.g.: expiration date for account and password, password strength, etc.); - have roles assigned to them, roles that define access and system	Must

	behavior.	
IMS_TECH_02_03	**Organizations; organization units; authorizations and access; access rights; software clients; workflows.** - system must support multiple organizations and their management; - system must support multiple organization units and their management; - system must support dedicated software clients and their management; - system must support setting a hierarchy of organization units and allow their management; - user accounts must have access to various system features allowed based on roles, user group, software type (server/client), action, organization and organization units; - access rights must support access rights templates; - system must support dedicated software clients for enrolment and issuing badges; - system must support workflows for transitioning badges between various states; - system must support configuring available options from the software clients and their behavior (actions, workflows, etc.).	Must
IMS_TECH_02_04	**Badges/cards features:** - system must allow creating badges for different person types (e.g. personnel, dependents, visitors, etc.); - system must support configurable hierarchies and links between identities with configurable rules; - system must allow different types of badges, configurable (e.g. with/without PIV, RFID/other access control technologies, etc.) - system must support smartcards, including smartcards approved by a National CIS Security Authority; - related to access control technologies, system must support multiple technologies – at least RFID and newer NIST Approved Algorithms; - system must allow design of badges (design can be per organizational unit, organization, per badge type, person type); - system must support stock management (add, transfer, trace) for the blank cards and cards characteristics management (serial number, RFID code, certificate); - system must support enrolment via biometrics capture (e.g. face, signature, etc.); - system must support face detection in biometrics images; - system must support badge management (importing personal information, enrolment, adding biometrics information, revoking, ending a badge); - system must support custom fields for badges; - values for badge's custom fields must be imported from external systems via interfaces or direct input; - system must be able to generate barcodes based on configurable badge information; - system must support reading RFID data from the badge and storing it	Must
IMS_TECH_02_05	**Reports and audit:** - all operations performed in the system (via web application or client	Must

	application) must be recorded/logged; - audit reports must be made available; - offer the possibility to search for performed operations; - reports for badges, users, software clients must be provided.	
IMS_TECH_02_05	**External e-mail system:** - system should support sending notifications to users or administrators on at least the following events: password recovery, password change, automated tasks completion	
Identity and Access Card Management System – Client features		
IMS_TECH_03_01	**The identity and access card management system must provide also a software client. The software client must:** - have a client-server architecture, preferably leveraging web services; - run on dedicated workstations (issuance kiosks); - allow issuance users to perform all operations needed for enrolment (data import, capture biometrics, print badge, verify badge, issue badge, revoke badge); - print badges to dedicated badge printers; - work with computer peripherals to read badge information (e.g. RFID, certificates, etc.) and configure badges (e.g. add certificates to badge, etc.); - be configurable by the server system in terms of types of badges supported, organizational units, workflows, captured data, input data, operations that can be performed by issuance user, etc.; - restrict users access based on user rights; - be able to print badges and generate them in PDF format; - be easily installable and upgradeable by using enterprise management tools.	Must
IMS_TECH_03_02	**The identity and access card management system must provide the option to capture/input data via the web browser, web application being used at least as a client system with limited features. The web application must:** - run in Edge web browser - allow issuance users to perform the identity management operations - allow issuance users to perform a part of the operations needed for enrolment (at least data import, capture biometrics, revoke badge); - be configurable in terms of organizational units, workflows, captured data, input data, operations that can be performed by user, etc.; - restrict users access based on user rights;	Must

Table 1 – Identity and Access Card Management System - Technical Requirements

Notes:

(1) For NATO PKI details, please refer to *NATO Certificate Policy*