Basic physical characteristics of ID

PWPW SA
Polska Wytwórnia Papierów Wartościowych S.A.
(Polish Security Printing Works)
ul. R. Sanguszki 1
00-222 Warszawa

Basic specification Polycarbonate ID-1

Date	Prepared by	Service for:
2024-07-16 – ver. 1.0	PWPW SA Polish Security Printing Works	AGETIA SERVICII PUBLICE

Below specification lists chief features of the card body and gives an overview of production and quality means. The final specification will be prepared based on actual artwork.

Products from the tender covered by the specification

The specification covers the following ID-1 polycarbonate product from the tender:

Polycarbonate blanks (cards) – **Identity card of the citizen of the Republic of Moldova (ID)**

Card body description

ID documents produced by PWPW SA are manufactured in ISO 14298 (Intergraf) certified production plant to meet stringent security measures as required for national level identification documents. Similarly the graphic design is adapted and processed in secure, separated from the Internet environment based on a special software that is available only for authorized users that design and manufacture ID documents and banknotes. As such final editable artwork is not available outside PWPW. Only simplified versions in .pdf or .jpg formats are shared with the authorized stakeholders of the project.

The card body of ID documents is a multi-layered structure made of PC material. Particular layers of the card are bound together in unified product by means of hot lamination process. Ready-made card is prepared for laser engraving personalization.

Basic physical features:

- Card dimensions: according to ISO/IEC 7810
- Contact interface: according to ISO/IEC 7816
- Contactless interface: according to ISO/IEC 14443
- Card is prepared for 10 years usage as defined in ISO/IEC 24789 standard

Planned structure of the ID document

The planned structure of the ID document will entail not less than 7 layers of polycarbonate film. Used polycarbonate substrate features no fluorescence under UV light.

Respective layers of the document are overprinted with offset printing with the usage of Pantone ink colors. It shall be emphasized that process CMYK colors are not used at all in printing of documents.

Listing of inks:

- Offset printing
  - on the front side:
    - minimum 8 visible colors (6 offset forms including iris printing, metameric ink pair and Pantone with UV fluorescence (2 forms with shift colors effect to A-B-A)) on the first layer (all in one polycarbonate layer)
    - minimum 4 invisible colors with UV/Bi UV fluorescence (3 offset forms including iris printing (with shift colors effect to A-B-A)) on the second layer (all in one polycarbonate layer)
  - on the back side:
    - minimum 8 visible colors (6 offset forms including iris printing, metameric ink pair and Pantone with UV fluorescence (2 offset forms with shift colors effect to A-B-A)) on the first layer (all in one polycarbonate layer)
    - minimum 3 invisible colors with UV /Bi UV fluorescence (2 offset forms including iris printing (with shift colors effect to A-B-A)) on the second layer (all in one polycarbonate layer)
- Silkscreen printing
  - on the front side:
    - OVI ink with UV fluorescence
  - on the back side:
    - iridescent ink.

The detailed specification of the card and positioning of particular security elements is elaborated after receiving the artwork.

The multilayer polycarbonate card body is prepared for laser engraving personalization, both flat and tactile.

Applicable standards

*Meeting the **ISO/IEC 7810** standard for ID-1 cards are fully prepared to be used as ID-1 size national level documents issued in line with **ICAO 9303** requirements for TD-1 documents.*

*Moreover the card bodies are tested internally at PWPW against the following set of standards **ISO/IEC 10373**, **ISO/IEC 7816** and **ISO/IEC 24789**.*

Security features

The following graphical security features would be applied. Values in square brackets indicate sections of the Technical Specification.

No.	Feature	Description
1	Iris Printing [7.4.2]	Iris printing is mainly an anti-copy security feature. On PC substrate iris printing is achievable only in offset printing. Printing of a continuous line with color transition is not possible to achieve with commercially available ink-jet and laser printers, as well as thermal-transfer printing. Any attempted imitation is easily detectable.
2	Line width modulation and interlaced guilloche lines [7.4.1]	The artwork provided by the issuer will be transformed for printing so as to secure anti-scanning and anti-coping protection. The transformation takes place in special software dedicated solely to design banknotes or ID documents and not available outside security zones in our production plant.

3	Guilloche Lines Print [7.4.1]	Guilloche lines are an anti-copy security feature which prevent from document counterfeiting and altering biographical data. The resolution required to produce sharp, thin and continuous lines is only achievable with offset printing, which is usually unavailable to counterfeiters. Creating state of the art guilloches design requires dedicated computer software which is accessible only for authorized security printers.
4	Microtexts [7.4.1]	Microtext (character height in positive not exceeding 0,25 mm and in negative – not exceeding 0,35 mm) is a text unreadable without magnifying glass. It can contain fonts of variable size to hinder unauthorized duplication. The artwork will include both positive and negative microtexts.
5	Optical Variable Ink with UV fluorescence [7.2.2]	OVI (representing the symbol of the electronic document) is a special type of security ink that displays a shift of color when observed at different angles. OVIs of specific color shifts are not available for non-secure applications and may be applied only by security printers.
6	Deliberate error [7.4.1]	Deliberate error or changing of a symbol in the microprinted text of the security background design is a security feature that makes it easier to recognize counterfeit documents. A counterfeiter who does not know the location of such a protection will not apply it in the fake document. It can be used to satisfy third level of protection.
7	UV Reactive Invisible Ink [7.2.5]	Inks that are invisible in daylight and visible in UV are suitable for protecting document's holder data and photo. In daylight they do not hinder data and photo verification. Graphic elements will include features listed in 7.2.5 of Technical Specification.
8	Hologram / DOVID [7.2.1]	Semi-transparent DOVID consisting of separate elements shall be distributed over a large area of the document to protect the main personalization areas on a discontinuous reflective layer. These elements will form inlays of foils without any residual materials between them, in order to allow the perfect fusion of the polycarbonate layers during the lamination process. Each DOVID element is applied as a discontinuous area (set of different elements with the smallest one being not bigger than 10 mm^2 and the biggest one will not exceed 200 mm^2 and the minimum distance between two graphical elements shall be 0,5 mm). DOVID items will display the following feature: - maintained in the same plane and angle of light reflection, the two distinct reflective colors of the DOVID will interchange at any 90° rotation. - by tilting "DOVID" up and down, part or the entire surface of the two colored reflective areas will simultaneously display animations in opposite directions. - a part of one of the two colored reflective areas forms an object that renders a positive 3D relief effect on the "DOVID" surface. The DOVID will be applied to a layer of polycarbonate to ensure adhesion with the body of the card, being placed in the structure of the card above the layer of biographical data engraved by laser. Area size: minimum 3l mm x 3l mm.
9	MLI on the back side [7.2.3]	MLI is a tactile security feature which contains fine structure of lenses, that is integrated into the card surface during the lamination step. For MLI to work properly, lenses must have a specific microstructure, i.e. strictly defined dimensions and smooth surface, adapted for card overlay composition, which is impossible to obtain by means of commonly available milling machines and without proper know-how. Further, MLI is personalized by means of laser engraving, i.e. images (portrait and birth date) are applied in such a way that each one is visible from a different angle. MLI can also contain pre-printed lenticular effect images made with

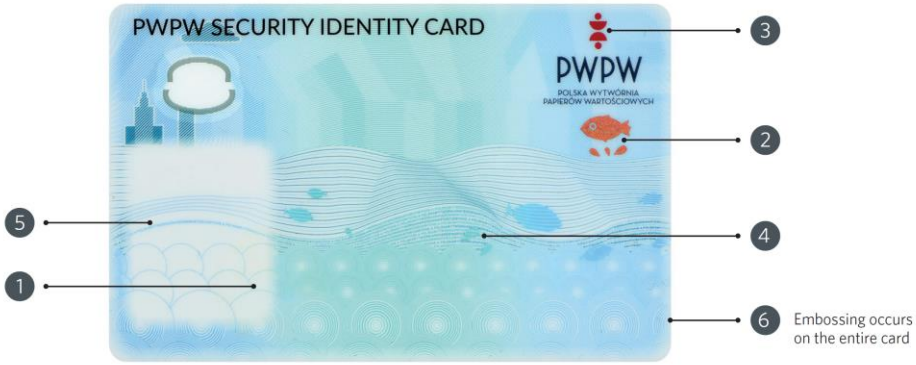
		offset printing technique. Repetition of the portrait and certain data enhances their protection and prevents forgery of the document.
10	Embossed card surface on both sides [7.2.4]	Obtaining sharp and fine convex shapes on the surface of the document is possible only by means of a special lamination process with specially prepared laminating plates, which is not available to counterfeiters. This thickness irregularity of the card surface profile protects against adding a film on top of the card with the impostor's data or photo substitution by means of scratching and milling. It also allows for easy verification of document authenticity by means of touch.
11	Card serial number [7.6]	Laser Engraved serial number. For full traceability no card without serial number leave our production plant. If needed the serial number can have barcode representation – e.g. CODE 128.
12	IR visible elements – Metameric effect [7.3]	Some elements of the image can be printed in such a way that they are partially visible in IR light. It does not influence the perception of the image in VIS light. Depending on application in the artwork it can be used as second or third level of protection.
13	Transparent window [7.2.6]	Security feature in the construction of the substrate, where part of non-transparent substrate is removed and/or replaced with transparent material. Achieving transparent window which changes its color according to the color of the background on which is viewed is possible by using O.V.M. materials. The window will change its color from blue (on light background) to red (on dark background), additionally there will be embedded image that will appear as a third color (yellow-green). Both, the background and the embedded image will be UV light reactive (yellow-green luminescence for the embedded image and red luminescence for the background). Size of the window area: 10 mm x 12 mm

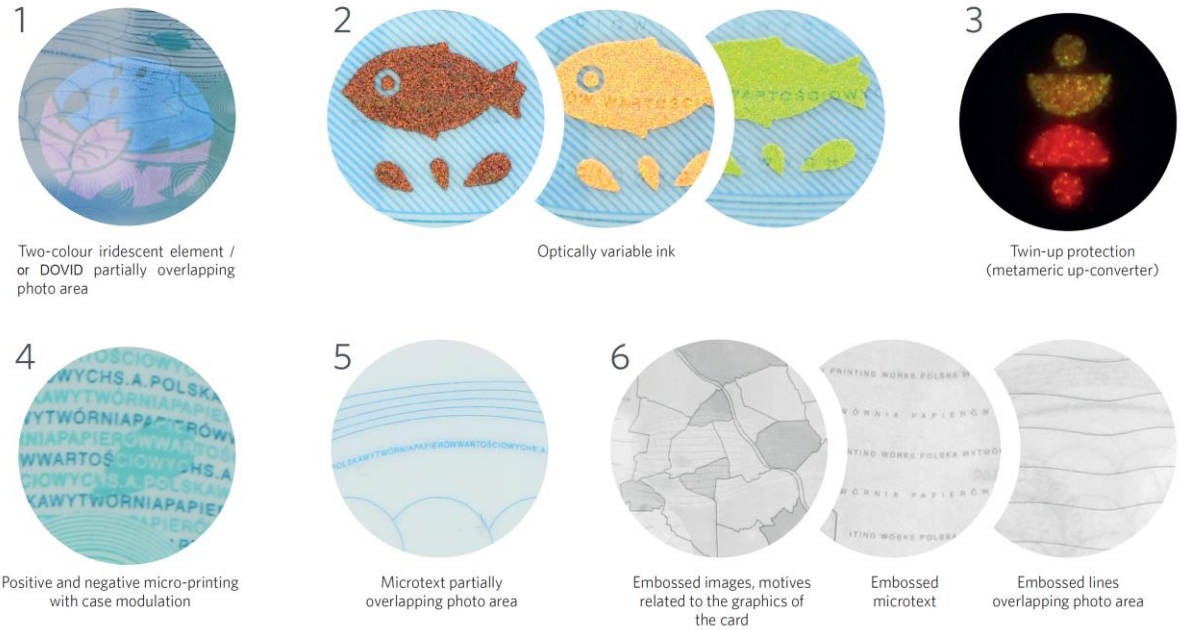
Exemplary usage of security features based on PWPW SA sample card

Below exemplary images are shown in order to present some the features listed in the above table.

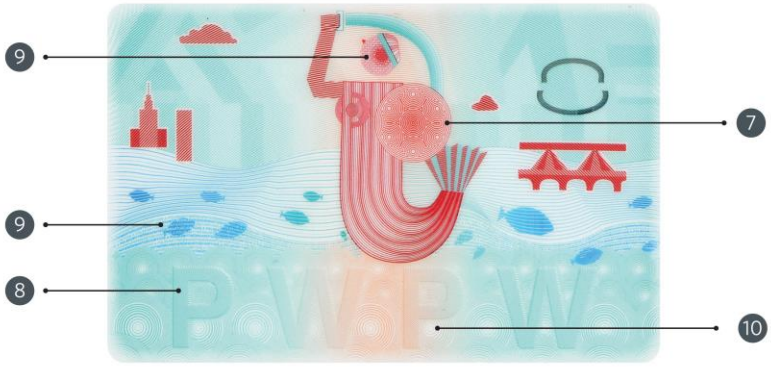
The following illustration is provided solely for the purpose of demonstrating PWPW's technical capabilities. Please note that this example ID-1 card does not meet all of the requirements outlined in Technical Specification.

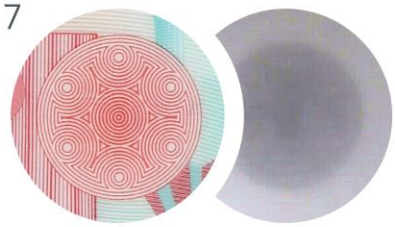
Front Side





Back Side




7

Metameric element printed with inks other than black


8

Relief background

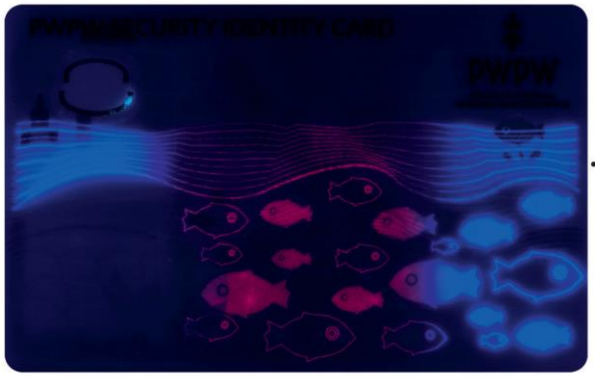

9

Positive and negative micro-printing with case modulation


10

Rainbow printing - guilloche lines

VIEW UNDER UV LIGHT



Rainbow printing visible in UV light

** Based on provided artworks PWPW propose adequate application of particular security elements pursuant to the requirements of the tender.

Additional information

Technologies applied and listed above basic security features will be adequately applied to provided artworks.

Moreover, in order to avoid ambiguities we do confirm the polycarbonate ID card will include security features as listed in tender documentation in the following documents:

- ST_MD_35_37603221_226_2024

Offered polycarbonate ID-1 cards are fully prepared for laser engraving personalization on the front and on the back side of the card.

Applied chip basic characteristics

Due to situation on the chip market and to ensure documents issuance continuity as an option we reserve the right, after consultancy with the Client, to use any of the following alternative Hardware and Software platform:

Option 1

Thales MultiApp ID v 5.1	
Chip	Thales Aquarius (EAL6+)
Free NVM	125Kb
Communication Interfaces	Contact interface fully compliant to ISO/IEC 7816-3 Contactless interface fully compliant to ISO/IEC 14443 - 3, 4 Very High Bit Rate (VHBR) option Support of Extended Length APDU (Tx 32/64kB - Rx 1kB/32kB in T=1 or T=CL) ATR fully configurable for integration in a legacy environment or to optimize the communication in a new system
Secure Embedded Software CC Certifications	ICAO: BAC EAL4+, BAC and EAC EAL5+, PACE EAL5+, PACE and EAC EAL5+ - November 2021 IAS: PP-SSCD EAL5+ - November 2021 Platform: JavaCard EAL 6+ Javacard 3.1 (EAL6+) / Global Platform 2.3.1 (EAL6+) / VM EAL7 Patch ability on the Field
PACE	Integrated, Generic and Chip Authentication Mapping DH 2048/ECDH 521

Supported Crypto	AES 256b, DES/3DES, RSA 2024 (up to 4K on demand) and ECC algorithms 512b
Supported protocols	Active Authentication, Chip Authentication, Terminal Authentication
Security Upgrade Management	YES
OS Type	Native OS
Supported Application	• Thales eTravel Applet for eResident-Permit o ICAO BAC (MRTD), o ICAO SAC/EAC (PACEv2), o Comply with BSI-TR 03110 • IAS Applet for o eID Application o QDS Application (Secure Signature Creation Device).

Common Criteria Certification

Certified Item	CC Level	Protection Profile
Thales Aquarius	EAL6+	BSI-PP-0084-2014
eTravel v3.1 on MAV5.1 BAC and AA activated	EAL4+	BSI-PP-055-2009
eTravel v3.1 on MAV5.1 PACE, EAC and AA activated	EAL5+	BSI-PP-0068-V2-2011-MA-01 BSI-PP-0056-V2-2012-MA-02
IAS Classic.5.2.1 on MultiApp v5.1	EAL5+	BSI-CC-PP-0059-2009-MA-02
IAS as QDSD	EAL5+	BSI-PP-0075-SSCD-P2 BSI-PP-0075-SSCD-P3 BSI-PP-0071-2012 BSI-PP-0072-2012 BSI-PP-0076-2012

Option 2

Thales MultiApp ID v 5.0

Chip	Infineon SLC37GDA512
Free NVM	125Kb
Communication Interfaces	Contact interface fully compliant to ISO/IEC 7816-3 Contactless interface fully compliant to ISO/IEC 14443 - 3, 4 Very High Bit Rate (VHBR) option Support of Extended Length APDU (Tx 32/64kB - Rx 1kB/32kB in T=1 or T=CL) ATR fully configurable for integration in a legacy environment or to optimize the communication in a new system
Secure Embedded Software CC Certifications	ICAO: BAC EAL4+, BAC and EAC EAL5+, PACE EAL5+, PACE and EAC EAL5+ - November 2021 IAS: PP-SSCD EAL5+ - November 2021 Platform: JavaCard EAL 6+ Javacard 3.1 (EAL6+) / Global Platform 2.3.1 (EAL6+) / VM EAL7 Patch ability on the Field
PACE	Integrated, Generic and Chip Authentication Mapping DH 2048/ECDH 521
Supported Crypto	AES 256b, DES/3DES, RSA 2024 (up to 4K on demand) and ECC algorithms 512b
Supported protocols	Active Authentication, Chip Authentication, Terminal Authentication
Security Upgrade Management	YES
OS Type	Native OS
Supported Application	• Thales eTravel Applet for eResident-Permit o ICAO BAC (MRTD), o ICAO SAC/EAC (PACEv2), o Comply with BSI-TR 03110 • IAS Applet for o eID Application o QDS Application (Secure Signature Creation Device).

Common Criteria Certification

Certified Item	CC Level	Protection Profile
Chip Platform SLC37GDA512	EAL6+	BSI-DSZ-CC-1107-2020
Thales Operation System	EAL6+	BSI-PP-099-V2-2020
eTravel v2.5 – MultiApp v5.0 BAC and AA activated	EAL4+	BSI-PP-055-2009
eTravel v2.5 – MultiApp v5.0 PACE, EAC and AA activated	EAL5+	BSI-PP-0068-V2-2011-MA-01 BSI-PP-0056-V2-2012-MA-02
eTravel v2.5 – MultiApp v5.0 BAC, EAC and AA activated	EAL5+	BSI-PP-0056-2009
IAS Classic.52 on MultiApp v5.0	EAL5+	BSI-CC-PP-0059-2009-MA-02
IAS as QDSD	EAL5+	BSI-PP-0075-SSCD-P2 BSI-PP-0075-SSCD-P3 BSI-PP-0071-2012 BSI-PP-0072-2012 BSI-PP-0076-2012

Software (for Option 1 and 2)

Middleware

IAS Classic Client offers the highest level of security by using public-key cryptography to store or update user identity credentials on a smartcard.

Overview

Classic Client is a middleware product that enables desktop applications to benefit from smart card based cryptographic solution in a PKI environment.

Classic Client offers the following services to desktop applications: authentication, digital signatures, confidentiality through symmetric key cryptography, support of public key cryptography and secure storage of keys and certificates.

Classic Client supports multi-factor authentication with your smart card ('something you have') in addition to biometric ('something you are') and/or PIN ('something you

know') credentials.

Capabilities

Secure access to Web Server via Client authentication using TLS

eMail encryption / signature with S/MIME applications

Smart card logon with Windows Operating System

Signature of documents

RSA and Elliptic curve public key cryptography

Onboard key generation

PIN management , PIN & PUK

Contactless secure mechanism support (anti-skimming)

Biometric credentials support

Standards / APIs

CryptoAPI – enabled for use with Microsoft Applications

Minidriver – enabled for use with Microsoft OS

PKCS #11 – enabled for use with Microsoft OS, MacOS and Linux Ubuntu

CyptoTokenKit framework – enabled for use with MacOS

PKCS#15 (ISO7816-15) card profile compliant

PKCS#1 v1.5 / v2.1

PKCS#12

PC/SC compliant

IAS Classic API – dedicated API with transparent channel and PKCS#15 browsing

Middleware SDK for Android and iOS

SDK for Android and iOS: called Classic Mobile Link (CML), a set of APIs to allow clients to interface with Thales Smartcards that comes with IAS classic to access its PKI and other cryptographic features.

CML V2.2 is a library that allows the user to access cryptographic services provided by the Smartcards that comes with IAS classic. The library provides card reader management in order to connect to different types of readers such as USB, NFC, and BLE (Bluetooth Low Energy).

Option 3

Microchip

NXP J3R252 JCOP 4.5 with middleware software

Basic characteristic

Commercial Type:	J3R252
12 NC:	TBD/TBC
OS:	JCOP 4.5
Interface:	CL/DIF
NVM Size [kB]:	250kB
SecID Applet:	ChipDoc v4 Edition 2
Others Technical Requirements:	MW, SEMS
Module	DIF 6 pins Au

Middleware

Middleware allowing, under any environment (Windows, Mac OS, Linux, iOS, Android), applications to:

- read identity documents (Passport, National Electronic Identity Card, ...)

- use PKI cards for:

• electronic signatures and/or document encryption/deciphering,

• implement strong authentication in browsers,

• secure access to the PC via Windows Logon,

• to secure the networks via VPN,

• to take safe remote control of a PC via Remote Desktop Protocol (RDP), ...

- manage the content of PKI cards

Quality control in PWPW plant

The quality control is accomplished based on the PN-ISO-2859-1 norm, titled "Sampling procedures for inspection by attributes", according to the sampling plan.

A PLAN OF THE ACCEPTANCE INSPECTION OF A LOT ACCORDING TO THE PN-ISO 2859-1 STANDARD

The batch of cards is verified in regard to is conformity, with Client-approved acceptance or pattern documents.

According to the abovementioned standard, developed test plan used during the receiving inspection, based the acceptable level of quality (AQL)

I. STAGES OF QUALITY INSPECTION

1) Inspection of cards for compliance with the graphic design contained in the project documentation or approved by the ordering patterns
2) Inspection according to the inspection plan based on the PN-ISO-2859-1 norm

II. A PLAN OF THE ACCEPTANCE INSPECTION OF A LOT ACCORDING TO THE PN-ISO 2859-1 norm

Inspection level II – standard for sample of the optimum size

Special level S3 – used when it is necessary to use a small sample, e.g. because tests are time-consuming, harmful or destructive

Normal inspection – standard at a given level In circumstances provided for by the PN-ISO 2859-1 it is acceptable to change the type of inspection onto a reduced or tightened one.

Sampling plan – single – a sample for the test is selected randomly and only once. The number of sample items inspected shall be equal to the sample size given by plan. If the number of nonconforming items found in the sample is equal to or less than the acceptance number, the lot shall be considered acceptable. If number of nonconforming items is equal to or greater than the rejection number, the lot shall be considered not acceptable.

Nonconformity classification:
Class A (critical defect) – those nonconformities significantly affect the product. They endanger document functionality or identification. The accepted AQL for this class has the value of 0.15 in the case of II inspection level and 0.4 in the case of the special S3 inspection level.

Class B (major defects) – those nonconformities can make it difficult to use the document or they will significantly change its appearance. The acceptable AQL for this class has the value of 1.5 and 2.5 in the case of inspection level II 2.5 and 4.0 in the case of the special S3 inspection level.

Class C (minor defects) – those nonconformities do not limit the use of the document but may negatively affect its appearance. The accepted AQL for this class has the value of 2.5 in the case of the inspection levels II.

The quality inspection shall be accordance with the sampling plan presented bellow (Table 1), appropriately for each characteristic selected for inspection. If the nonconformities for an inspected characteristic do not exceed the number (i.e. AC), the characteristic fulfils the quality criteria. If the AC acceptable number for any characteristic be exceeded, the lot does not fulfil the requirements.

Table 1 – Quality acceptance plan for a product lot

Item	The inspected characteristic	The object of the inspection	Inspection level	AQL	Notes
1	Identification and functional element of the card in visible light (e.g. graphics, texts, security features, numbering, embossing, hologram, MLI, numbering, window, microprocessor)	The presence	II	0,15	Presence of elements consistent with the pattern
		Appearance and colours	II	2,5	The appearance and colors of all elements accordance with the pattern and the border patterns
		Positioning	II	1,5	According to the technical specification
		Appearance and readability microtext	S3	4	Visual assessment
2	The appearance and representation security elements in print and application in UV, IR and up-converting lights	The presence	S3	0,4	Presence of elements consistent with the pattern
		Appearance and colors	S3	2,5	Elements active in UV and up-converting light are checked for correct reproduction, color and intensity of UV light consistent with the pattern. Visibility/invisibility in IR light are checked for correct reproduction consistent with the pattern.
3	Format, card edges	Card dimensions, appearance in the edge area	II	2,5	According to the technical specification

Table 2 – positioning tolerance of individual elements

No.	Parameter	Tolerance	Remarks
1	Matching offset printed elements against each other	top, bottom +/-0,2 mm left, right +/-0,2 mm	Visual inspection, magnifying glass, length measuring unit
2	Positioning offset printed elements and silkscreen printed elements against the edge of the card	top, bottom +/- 1,0 mm left, right +/- 1,0 mm	Against the edge of the card (check based on the template)
3	MLI	top, bottom +/- 1,0 mm left, right +/-1,0 mm	Against the edge of the card (check based on the template)
4	Hologram	top, bottom +/- 1,5 mm left, right +/- 1,5 mm	Against the edge of the card (check based on the template)
5	Numbering	top, bottom +/- 1,0 mm left, right +/-1,0 mm	Against the edge of the card (check based on the template)
6	Size	According ISO 7810 i.e.: width 85,6 mm, tolerance 85,47÷ 85,72 mm height 54,0 mm, tolerance 53,92÷54,03 mm thickness 0,76 mm, tolerance 0,68 ÷ 0,84 mm	Against the edge of the card (check based on the template)

Checking the quality of execution of card is conducted according to above-mentioned Quality acceptance plan, and criteria in Tables 1 and 2, respectively for each of the evaluated elements. Existing non-compliance are not summed for comparison with number of eligible AC. Exceeding the number of eligible AC is checked only for each properties alone.