

2D Barcode Content	Document Number Crosscheck	Near-Infrared Response
2D Barcode Read	Document Orientation	Optically Variable Ink Pattern
Active Authentication	DSC Certificate Valid	Optically Variable Ink Response
Application Date Crosscheck	Expiration Date Check Digit	Overlay Pattern
Basic Access Control	Expiration Date Crosscheck	Overlay Response
Birth Date Check Digit	Expiration Date Valid	Passive Authentication
Birth Date Crosscheck	Full Name Crosscheck	Personal Number Check Digit
Birth Date Valid	Given Name Crosscheck	Personal Number Crosscheck
Chip Authentication	Image Tampering Check	Photo Printing
Chip Certificate Chain Validity Check	Issue Date Crosscheck	Series Date Valid
Composite Check Digit	Issue Date Valid	Sex Crosscheck
Contactless Chip Content	Issuing State Valid	SOD Signature Check
Contactless Chip Presence	Laser Perforation	Substrate Printing
Contactless Chip Read	Layout Valid	Supplemental Access Control
Control Number Crosscheck	Magstripe Content	Surname Crosscheck
COM/SOD Crosscheck	Magstripe Presence	Terminal Authentication
Validate Chip Data Group	Magstripe Read	Ultraviolet Material Response
Document Classification	MRZ Crosscheck	Ultraviolet Pattern
Document Crosscheck Aggregation	Nationality Code Crosscheck	Ultraviolet Response
Document Expired	Nationality Valid	Visible Color Response
Document Number Check Digit	Near-Infrared Pattern	Visible Pattern

Authentication Test	Description	Possible Cause of Failure
2D Barcode Content	Checks the contents of the (two-dimensional) 2D barcode on the document.	A 2D barcode was: • read but could not be correctly decoded, or • incorrectly encoded (either inadvertently due to a manufacturing problem or intentionally), or • a new barcode format that is currently not supported by the software version.
2D Barcode Read	Verifies that the (two-dimensional) 2D barcode on the document was read successfully.	A 2D barcode could not be read successfully because it is either: • dirty or in poor condition • covered by a foreign material (such as a sticker), or • invalid or a poor-quality replication of an authentic barcode.
Active Authentication	Verifies that the contactless chip in the document is genuine and that the tamper-resistant key in the contactless chip was not substituted.	Visually inspect the back cover of the document for tampering. The contactless chip in the document is either: • not genuine, or • the digital signature verification of a tamper-resistant key in the contactless chip fails. Another cause could be that the document was prematurely removed from the reader.
Application Date Crosscheck	Compares the application date to information contained in one or more visible or machine-readable application date fields.	The application date on one or more data sources doesn't match.
Basic Access Control	Verifies that secure communication with the contactless chip in the document was established.	Secure communication between the contactless chip and the inspection system was not established.
Birth Date Check Digit	Verifies that the visible birth date is the same as the check digit from the birth date check digit in the MRZ.	Any misread characters in the MRZ can cause a failure of the birth date check digit.
Birth Date Crosscheck	Checks the birth date field against information contained in one or more visible or machine-readable birth date fields.	The birth date in one or more visible or machine-readable data sources doesn't match.
Birth Date Valid	Verifies that the birth date could be read, is in the expected format, and occurs on or before the current date and not outside a reasonable range.	The birth date is invalid because it is either not in the expected format, or it is on or before the current date or outside a reasonable range.

Authentication Test	Description	Possible Cause of Failure
Chip Authentication	Verifies that the contactless chip in the document is authentic.	The Certificate Chain used to sign the chip data is invalid.
Chip Certificate Chain Validity Check	Verifies that the Chip Certificate Chain used to sign the chip data is valid.	The Chip Certificate Chain used to sign the chip data is invalid and could indicate an attempt to digitally alter or partially replace the chip data.
Composite Check Digit	Performs a checksum validation on the MRZ.	Any misread characters in the MRZ can cause a failure of the Composite Check Digit test.
Contactless Chip Content	Checks the contents of the contactless chip in the document.	A contactless chip was detected and read but can't be correctly decoded.
Contactless Chip Presence	Checks for the presence of a contactless chip in the document.	A contactless chip was not detected.
Contactless Chip Read	Verifies that the contactless chip in the document was read successfully.	A contactless chip was detected but couldn't be read successfully.
Control Number Crosscheck	Compares the control number to information contained in one or more visible or machine-readable control number fields.	The information contained in one or more control number fields doesn't match. The control number may have been misread due to dirt or wear. Confirm that the data from all visible sources match and are free of obstructions.
COM/SOD Crosscheck	Checks that the same data-groups exist in the COM and SOD fields.	The same data-groups do not exist in the COM and SOD fields.
Validate Chip Data Group	Verifies that the chip data group is valid.	The chip data isn't authentic or couldn't be read correctly.
Document Classification	Verifies that the document type is supported and can be fully authenticated.	The document isn't recognized as a supported document type or the document type can't be fully authenticated. The document should be examined manually. The document may be either: • a fraudulent (counterfeit) document • a valid document that is significantly worn or damaged, or • the document is a new or different type that is not yet supported by <i>Acuant</i> Document Library.

Authentication Test	Description	Possible Cause of Failure
Document Crosscheck Aggregation	Checks the document against the information contained in one or more visible or machine-readable document fields.	The document on one or more data sources doesn't match. The machine-readable data may be from a totally different person from what is represented on the front of the card. This may indicate: • a tampering attempt to the visible data regions • a fraudulent (counterfeit) document, or • an accidental scanning of the front and back from two different documents.
Document Expired	Verifies that the document expiration date doesn't occur before the current date.	The document has expired.
Document Number Check Digit	Compares the machine-readable document number check digit to the calculated check digit from the visible document number.	Any misread characters in the MRZ can cause a failure of the document number check digit.
Document Number Crosscheck	Checks the document number against the information contained in one or more visible or machine-readable document number fields.	The document number on two or more data sources do not match. The document number may have been misread due to dirt or wear. Confirm that the data from all visible sources match and are free of obstructions.
Document Orientation	Checks that the document was presented in the correct orientation (<i>horizontal vs. vertical</i>).	The document is presented in the wrong orientation (vertically vs. horizontally) which can falsely indicate the absence of a magnetic stripe on some documents.
DSC Certificate Valid	Verifies that time is within the Document Signer Certificate (DSC) validity period.	The issuer has indicated that the type can no longer be considered secure on the current date.
Expiration Date Check Digit	Checks the expiration date against information contained in the calculated expiration date check digit from the machine-readable zone (MRZ).	The visible expiration date doesn't match the expiration date check digit on the MRZ.
Expiration Date Crosscheck	Compares the visible expiration date field to one or more machine-readable expiration date fields.	The visible expiration date on two or more of these sources doesn't match.
Expiration Date Valid	Verifies that the document expiration date is valid, in the expected format, and occurs after the issue and/or birth dates.	The document expiration date is invalid because it either: • is not in the expected format, • occurs before the issue date, or • occurs before the birth date.

Authentication Test	Description	Possible Cause of Failure
Full Name Crosscheck	Checks the full name against the information contained in one or more visible or machine-readable full name fields.	The full name field on two or more of these sources doesn't match. The full name may have been misread due to dirt or wear. Confirm that the data from all visible sources match and are free of obstructions.
Given Name Crosscheck	Checks the given name against information contained in one or more visible or machine-readable given name fields.	The given name on two or more of these sources doesn't match.
Image Tampering Check	Examines a document image for evidence of tampering or digital manipulation.	The document image shows evidence of tampering or digital manipulation.
Issue Date Crosscheck	Checks the issue date against the information contained in one or more visible or machine-readable issue date fields.	The issue date on two or more of these sources doesn't match.
Issue Date Valid	Verifies that the document issue date is valid and in the expected format.	The issue date is invalid because it either: • is not in the expected format, • contains a date that occurs in the future, or • occurs after the expiration date.
Issuing State Valid	Verifies that the issuing state is valid by checking it against the list of standard state codes.	The issuing state is invalid because it was either: • misread, or • doesn't appear on the list of standard state codes.
Laser Perforation	Verifies the presence of a laser perforation feature on the document.	No laser perforation was detected.
Layout Valid	Verifies that the layout (relative positions of features on the document are within the normal area) of the document is correct.	The layout is invalid because either the document was: • moving or slipped during the capture, or • excessively worn or damaged.
Magstripe Content	Checks the contents of the magnetic stripe (magstripe) on the document.	A magstripe was detected and read but can't be correctly decoded because the magstripe was either: • dirty or in poor condition, or • the contents of the magstripe were incorrectly encoded (either inadvertently due to a manufacturing problem or intentionally).

Authentication Test	Description	Possible Cause of Failure
Magstripe Presence	Checks for the presence of a magnetic stripe (magstripe) on the document.	No magstripe was detected.
Magstripe Read	Verifies that the magnetic stripe (magstripe) on the document was read successfully.	A magstripe was detected but could not be read successfully because it is either: - dirty or in poor condition, or - covered by a foreign material (such as a sticker).
MRZ Crosscheck	Compares the machine-readable zone (MRZ) printed on the document to the MRZ on the contactless smart card.	The MRZ printed on the document does not match the MRZ on the contactless smart card.
Nationality Code Crosscheck	Checks the nationality code field to one or more visible or machine-readable nationality code fields.	The nationality code on two or more data sources doesn't match.
Nationality Valid	Verifies that the nationality code is legible and that it is on the list of standard nationality codes.	The nationality code is invalid because it either: - may have been misread, or - doesn't appear on the list of standard nationality codes.
Near-Infrared Pattern	Verifies that a security feature, visible in the near-infrared spectrum, is present and in an expected location on the document.	The near-infrared pattern is either not present or not in the expected location on the document. The document may have been: - moved during the capture, or - excessively worn or damaged.
Near-Infrared Response	Verifies that text, photos, and other features on a region of the document respond as expected when viewed under near-infrared light to determine whether: - the photo has not been substituted - the document is authentic (not counterfeit), or - the document has not been tampered with or modified	The document does not respond correctly when viewed under near-infrared light. If the region of interest is within the photo area, confirm that the photo has not been tampered with or substituted. If the region of interest is over data, confirm that the data has not been tampered with. The document may have been: - moved during the capture, or - excessively worn or damaged.
Optically Variable Ink Pattern	Verifies the presence of an optically variable ink pattern on the document. Note: The pattern should vary in color (but not shape) as you tilt the document.	No optically variable ink pattern was detected on the document. The document may have been: - moved during the capture, or - excessively worn or damaged.

Authentication Test	Description	Possible Cause of Failure
Optically Variable Ink Response	Verifies the response of an optically variable ink pattern on the document.	The document may have been: • removed from the reader authenticator before the image could be captured • moved during the capture, or • excessively worn or damaged.
Overlay Pattern	Checks the document to verify the presence of a pattern on the document overlay and verifies the integrity of the document overlay that seals the document in order to verify that: • the photo has not been substituted • the document is authentic (not counterfeit), or • the document has not been tampered with or modified.	The document may have been: • removed from the reader authenticator before the image could be captured • moved during the capture, or • excessively worn or damaged.
Overlay Response	Verifies that a region of the document overlay or laminate material responds as expected.	A region of the document overlay or laminate material did not respond as expected. The document may have been: • removed from the reader authenticator before the image could be captured • moved during the capture, or • excessively worn or damaged.
Passive Authentication	Verifies that the contactless chip in the document is: • authentic (not counterfeit) • has not been tampered with or modified.	The digital signatures of the data in the contactless chip are either invalid or could not be validated.
Personal Number Check Digit	Validates the visible personal number check digit by comparing it to a calculated check digit from the visible personal number element.	The personal number check digit doesn't match the visible personal number.
Personal Number Crosscheck	Checks the personal number against the information contained in the visible or machine-readable personal number fields.	The machine-readable personal number doesn't match the visible personal number.

[Back to Top](#)

Authentication Test	Description	Possible Cause of Failure
Photo Printing	Verifies that a detailed photo printing technique was used, and a photo can be used to verify that: - the photo has not been substituted - the document is authentic (not counterfeit), or - the document has not been tampered with or modified.	This test may fail on an authentic document if the document is: - out of focus due to warping - moved during the capture, or is - excessively worn or damaged.
Series Date Valid	Verifies that the referenced series date (such as issue date or expiration date) on the document occurs within the published or known expected range for the document series.	The referenced series date on the document doesn't occur within the published or known expected range for the document series.
Sex Crosscheck	Checks the sex against information contained in the visible or machine-readable sex fields.	The sex fields on two or more of these sources do not match.
SOD Signature Check	Verifies that the SOD signature is valid.	The SOD signature is invalid.
Substrate Printing	Verifies that a detailed printing technique, which can be used to detect a counterfeit document, was used when the blank document was created.	The document may have been: - moved during the capture, or is - excessively worn or damaged.
Supplemental Access Control	Verifies that secure communication with the contactless chip in the document was established.	Secure messaging with the contactless chip could not be established.
Surname Crosscheck	Checks the surname against the information contained in the visible and machine-readable surname field.	The surname field on two or more of these sources doesn't match.
Terminal Authentication	Verifies whether the system can to read sensitive data from the contactless chip in the document.	- Secure messaging with the contactless chip could not be established, or - the request to digitally sign an external request was not completed with a valid inspection system key.

[Back to Top](#)

Authentication Test	Description	Possible Cause of Failure
Ultraviolet Material Response	Confirms that the ultraviolet response for the entire document is correct for that type of document and verifies that the material of the document responds as expected when viewed under ultraviolet light • If the region of interest is within the photo area, confirms that the photo has not been tampered with or substituted • If the region of interest is over data, confirms that the data has not been tampered with or modified. Note: Certain types of documents should not respond under ultraviolet light and should appear as a dark image. Conversely, tampered or counterfeit documents may appear bright blue.	The document could be: • excessively worn or damaged, or • tampered with or modified.
Ultraviolet Pattern	Verifies that a security feature, visible in the ultraviolet spectrum, is present and in an expected location on the document	The ultraviolet pattern was either not detected or not in the expected location on the document. The feature may have been omitted from the document due to a manufacturing or printing error. The document may have been: • removed from the reader before the UV image could be captured • moved during the capture, or • excessively worn or been subject to treatment that may have worn off or removed the UV ink.
Ultraviolet Response	Checks that a region of the document responds as expected when viewed under ultraviolet light. Confirms that the area of the test has not been tampered with, and that it was made using the correct material. Note: The material should not respond with a bright blue color.	The document may contain: • a sticker placed on the tested part of the document, or • a responsive stain from whitening agents (such as laundry detergent or glue).

Authentication Test	Description	Possible Cause of Failure
Visible Color Response	Verifies that the material of the document responds as expected when viewed under white light. • If the region of interest is within the photo area, confirms that the photo has not been tampered with or substituted • If the region of interest is over data, confirms that the data has not been tampered with	The document may have been: • moved during the capture • excessively worn or damaged • captured in poor lighting conditions, or • captured with a device that was not calibrated correctly.
Visible Pattern	Verifies that a security feature in the visible spectrum is present and in an expected location on the document.	The visible pattern was either not detected or not in the expected location on the document. The document may have been: • moved during the capture, or • is excessively worn or damaged.

[Back to Top](#)