

## Ergebnis der automatisierten Ausweisprüfung

Stand: Juni 2017

Kategorie	Ergebnis
Optische Prüfungen	mögliche Werte siehe unten
Elektronische Prüfungen	mögliche Werte siehe unten
Kombinierte Prüfung	mögliche Werte siehe unten
MLZ Prüfung	mögliche Werte siehe unten
Erweiterte Elektronische Prüfung	mögliche Werte siehe unten

## Prüfungsergebnisse

Ergebnis	Bedeutung
Erfolgreich	(Teil-)Prüfung wurde vollständig durchgeführt, Prüfergebnis positiv
Fehlgeschlagen	(Teil-)Prüfung wurde vollständig durchgeführt, Prüfergebnis negativ
Undefiniert	es liegt kein eindeutiges Prüfergebnis vor, diesen Fall gibt es nur bei der Chipprüfung bei fehlenden Zertifikaten
Nicht anwendbar	(Teil-)Prüfung nicht möglich (z.B. Chipprüfung, wenn Dokument keinen Chip hat)
Abgebrochen	(Teil-)Prüfung durch den Benutzer oder durch einen Systemfehler abgebrochen

## Statusübersicht über die Auffälligkeiten bei den Prüfungen mit den Ausweiselesegeräten

Stand: Juni 2017

Kategorie	Prüfung	Teilprüfung	Weitere Informationen	Bedeutung	Ergänzende Informationen	Quelle
Optische Prüfungen	<b>MRZConsistencyCheck</b>			Zusammenfassung der nachfolgenden Teilprüfungen: MRZ Prüffzifferncheck		
Optische Prüfungen	MRZConsistencyCheck	MRZCheckDigitComposite		Prüffzifferncheck für die gesamte MLZ		
Optische Prüfungen	MRZConsistencyCheck	MRZCheckDigitDocumentNumber		Prüffzifferncheck für die Dokumentennummer		
Optische Prüfungen	MRZConsistencyCheck	MRZCheckDigitDateOfExpiry		Prüffzifferncheck für das Ablaufdatum		
Optische Prüfungen	MRZConsistencyCheck	MRZCheckDigitDateOfBirth		Prüffzifferncheck für das Geburtsdatum		
Optische Prüfungen	MRZConsistencyCheck	MRZCheckDigitOptionalData		Prüffzifferncheck für die optionalen Daten		
Optische Prüfungen	<b>SpectrallySelectiveVerification</b>			Zusammenfassung der nachfolgenden Teilprüfungen: Optische Merkmalsprüfungen auf dem Weisslicht-, Infrarot- und UV-Bild		
Optische Prüfungen	SpectrallySelectiveVerification	BasicCheckResult	Muster: bspw. "pattern1", Typ: bspw. "IR-CROPPED", Position: bspw. "BACK"	Optische Merkmalsprüfungen (dokumentspezifisch); angezeigt werden neben dem "Merkmalstest" (pattern 1-n) der Typ (Weisslicht, Infrarot oder UV) und die Position (Front (= Lichtbildseite) oder Back		
Elektronische Prüfungen	<b>ChipAuthenticityCheck</b>			Zusammenfassung der nachfolgenden Teilprüfungen: Überprüfung der Echtheit des Chips	Fehlgeschlage Prüfungen aus dieser Prüfgruppen haben die Ursache entweder in defektem Ausweis-/Reisepass-Chip oder manipuliertem Chip	
Elektronische Prüfungen	ChipAuthenticityCheck	AA		Überprüfung der Echtheit des Chips mit Active Authentication,	Active Authentication authenticates the contactless IC by signing a challenge sent by the IFD (inspection system) with a private key known only to the IC. For this purpose the contactless IC contains its own Active Authentication Key pair (KPrAA and KPuAA). A hash representation of Data Group 15 (Public Key (KpuAA) info) is stored in the Document Security Object (SOD) and therefore authenticated by the issuer's digital signature. The corresponding Private Key (KPrAA) is stored in the contactless IC's secure memory. By authenticating the visual MRZ (through the hashed MRZ in the Document Security Object (SOD)) in combination with the challenge response, using the eMRTD's Active Authentication Key Pair (KPrAA and KPuAA), the inspection system verifies that the Document Security Object (SOD) has been read from the genuine contactless IC, stored in the genuine eMRTD. Active Authentication requires processing capabilities of the eMRTD's contactless IC.	<a href="https://www.icao.int/publications/Documents/9303_p11_cons_en.pdf">vgl:https://www.icao.int/publications/Documents/9303_p11_cons_en.pdf</a>
Elektronische Prüfungen	ChipAuthenticityCheck	CA		Überprüfung der Echtheit des Chips mit Chip Authentication	<b>Chip Authentication</b> The Chip Authentication Protocol is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the MRTD chip. The main differences to Active Authentication are: • Challenge Semantics are prevented because the transcripts produced by this protocol are nontransferable. • Besides authentication of the MRTD chip this protocol also provides strong session keys. Details on Challenge Semantics are described in Appendix C. The static Chip Authentication Key Pair(s) MUST be stored on the MRTD chip. • The private key SHALL be stored securely in the MRTD chip's memory. • The public key SHALL be provided as SubjectPublicKeyInfo in the ChipAuthenticationPublicKeyInfo structure (see Section 9.2.6). The protocol provides implicit authentication of both the MRTD chip itself and the stored data by performing Secure Messaging using the new session keys. As the eMRTD Application is selected as a result of the chip access procedure, Chip Authentication is performed in the eMRTD Application.	<a href="https://www.icao.int/publications/Documents/9303_p11_cons_en.pdf">vgl. auch ,https://www.icao.int/publications/Documents/9303_p11_cons_en.pdf</a>
Elektronische Prüfungen	<b>ChipSignatureCheck</b>			Zusammenfassung der nachfolgenden Teilprüfungen: Überprüfung der Sicherheitsobjekte EF.SOD, EF.CARDSecurity und EF.ChipsSecurity	Hashwerte aller Datengruppen sowie elekt. Signatur über diese Hashwerte.	siehe auch <a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03135/BSI-TR-03135.pdf?__blob=publicationFile">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03135/BSI-TR-03135.pdf?__blob=publicationFile</a>
Elektronische Prüfungen	ChipSignatureCheck	SecurityFile	Typ: bspw. "EF_SOD"	Überprüfung der Sicherheitsobjekte EF.SOD		
Elektronische Prüfungen	<b>IssuerCertificatesCheck</b>			Zusammenfassung der nachfolgenden Teilprüfungen: Überprüfung des Ausstellerzertifikats		
Elektronische Prüfungen	IssuerCertificatesCheck	SecurityFile	Typ: bspw. "EF_SOD"	Überprüfung der Signatur des DS Zertifikats nach BSI-TR		
Elektronische Prüfungen	<b>IntegrityCheck</b>			Zusammenfassung der nachfolgenden Teilprüfungen: Überprüfung der Integrität der Daten		
Elektronische Prüfungen	IntegrityCheck	EF_SODvsEFCOMCheck		Vergleich der Daten aus EFSOD mit den Daten aus EFCOM	Header and Data Group Presence Information EF.COM EF.COM is located in the eMRTD application (Short File Identifier = 0x1E) and contains LDS version information, Unicode version information and a list of the Data Groups that are present for the application. The eMRTD application must have only one file EF.COM that contains the common information for the application.	<a href="https://www.icao.int/publications/Documents/9303_p10_cons_en.pdf">https://www.icao.int/publications/Documents/9303_p10_cons_en.pdf</a> (Seite 19) siehe auch <a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03135/BSI-TR-03135.pdf?__blob=publicationFile">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03135/BSI-TR-03135.pdf?__blob=publicationFile</a>

Elektronische Prüfungen	IntegrityCheck	DataGroupIntegrityCheck		Überprüfung der Integrität der Daten für alle Datengruppen (DG1 bis DG16)	Data Group 1 — Machine Readable Zone Information (REQUIRED) Data Group 2 — Encoded Identification Features — Face (REQUIRED) Data Group 3 — Additional Identification Feature — Finger(s) (OPTIONAL) Data Group 4 — Additional Identification Feature — Iris(es) (OPTIONAL) Data Group 5 — Displayed Portrait (OPTIONAL) Data Group 6 — Reserved For Future Use Data Group 7 — Displayed Signature or Usual Mark (OPTIONAL) Data Group 8 — Data Feature(s) (OPTIONAL) Data Group 9 — Structure Feature(s) (OPTIONAL) Data Group 10 — Substance Feature(s) (OPTIONAL) Data Group 11 — Additional Personal Detail(s) (OPTIONAL) Data Group 12 — Additional Document Detail(s) (OPTIONAL) Data Group 13 — Optional Details(s) (OPTIONAL) Data Group 14 — Security Options (CONDITIONAL) Data Group 15 — Active Authentication Public Key Info (CONDITIONAL) Data Group 16 — Person(s) to Notify (OPTIONAL)	siehe auch <a href="https://www.icao.int/publications/Documents/9303_p10_cons_en.pdf">https://www.icao.int/publications/Documents/9303_p10_cons_en.pdf</a> <a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03135/BSI-TR-03135.pdf?__blob=publicationFile">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03135/BSI-TR-03135.pdf?__blob=publicationFile</a> <a href="http://winwiki.wi-fom.de/index.php/Der_neue_Reisepass_im_Lichte_des_Datenschutzes">http://winwiki.wi-fom.de/index.php/Der_neue_Reisepass_im_Lichte_des_Datenschutzes</a>
Elektronische Prüfungen	IssuingCountryComparison			Vergleich Ausstellerland aus dem DS-Zertifikat mit dem Ausstellerland aus der DG-1 vom Chip		
<b>Kombinierte Prüfung</b>	<b>DateOfExpiryCheck</b>			<b>Zusammenfassung der kombinierten Prüfungen nach BSI-TR</b>		
Kombinierte Prüfung	DateOfExpiryCheck	daysStillValid		Überprüfung des Ablaufdatums der MRZ		
Kombinierte Prüfung	MRZDG1Check			Vergleich der Daten aus der maschinenlesbaren Zone mit den Daten vom Chip		
Kombinierte Prüfung	MRZvsVIZCheck			Vergleich der Daten aus der maschinenlesbaren Zone mit den Daten aus der Visual Inspection Zone		
<b>MLZ Prüfung</b>	<b>MrzAdvancedCheckResult</b>			<b>Zusammenfassung der BDR (Bundesdruckerei) spezifischen Überprüfungen der maschinenlesbaren Zeile</b>		
MLZ Prüfung	MrzAdvancedCheckResult	MrzCharacterAlignment		Prüft, ob die Zeichen der MLZ eine feste Zeichenbreite aufweisen		
MLZ Prüfung	MrzAdvancedCheckResult	MrzHorizonAlignment		Prüft, ob die Zeilen der MLZ parallel ausgerichtet sind		
MLZ Prüfung	MrzAdvancedCheckResult	MrzVerticalAlignment		Prüft, ob die Zeilen der MLZ genau übereinander liegen		
MLZ Prüfung	MrzAdvancedCheckResult	MrzFont		Prüft, ob die Zeichen der MLZ der OCR-B Schriftart entsprechen		
MLZ Prüfung	MrzAdvancedCheckResult	DocumentTypeValidity		Überprüfung des Dokumententyps auf Plausibilität		
MLZ Prüfung	MrzAdvancedCheckResult	IssuingStateValidity		Überprüfung des Ausstellerlands auf Plausibilität		
MLZ Prüfung	MrzAdvancedCheckResult	DateOfExpiryValidity		Prüft, ob das Ablaufdatum ICAO konform ist und ob die Zahlenwerte für Tag, Monat und Jahr in einem gültigen Bereich liegen.		
MLZ Prüfung	MrzAdvancedCheckResult	GenderValidity		Überprüfung des Geschlechts auf Plausibilität		
MLZ Prüfung	MrzAdvancedCheckResult	NationalityValidity		Überprüfung der Nationalität auf Plausibilität		
MLZ Prüfung	MrzAdvancedCheckResult	DocumentNumberValidity		Überprüfung der Dokumentennummer auf Plausibilität		
MLZ Prüfung	MrzAdvancedCheckResult	SurnameValidity		Überprüfung des Nachnamens auf Plausibilität		
MLZ Prüfung	MrzAdvancedCheckResult	GivenNamesValidity		Überprüfung des Vornamens auf Plausibilität		
MLZ Prüfung	MrzAdvancedCheckResult	DateOfBirthValidity		Prüft, ob das Ablaufdatum ICAO konform ist und ob die Zahlenwerte für Tag, Monat und Jahr in einem gültigen Bereich liegen.		
MLZ Prüfung	MrzAdvancedCheckResult	OptionalDataValidity		Überprüfung der optionalen Daten auf Plausibilität		
MLZ Prüfung	MrzAdvancedCheckResult	CheckDigitCompositeValidity		Überprüfung der Gesamtprüfziffer auf Plausibilität		
MLZ Prüfung	MrzAdvancedCheckResult	CheckDigitDateOfBirthValidity		Überprüfung der Prüfziffer für das Geburtsdatum auf Plausibilität		
MLZ Prüfung	MrzAdvancedCheckResult	CheckDigitDateOfExpiryValidity		Überprüfung der Prüfziffer für das Ablaufdatum auf Plausibilität		
MLZ Prüfung	MrzAdvancedCheckResult	CheckDigitDocumentNumberValidity		Überprüfung der Prüfziffer für die Dokumentennummer auf Plausibilität		
MLZ Prüfung	MrzAdvancedCheckResult	CheckDigitOptionalDataValidity		Überprüfung der Prüfziffer für die optionalen Daten auf Plausibilität		
<b>Erweiterte Elektronische Prüfung</b>	<b>ElectronicAdvancedCheckResult</b>			<b>Zusammenfassung der BDR spezifischen Überprüfungen des Chips</b>		
Erweiterte Elektronische Prüfung	ElectronicAdvancedCheckResult	CfiChecks		Überprüfung der Zertifikatsrückrufliste	<a href="https://en.wikipedia.org/wiki/Certificate_revocation_list">https://en.wikipedia.org/wiki/Certificate_revocation_list</a>	
Erweiterte Elektronische Prüfung	ElectronicAdvancedCheckResult	ChipFoundAsExpected		Überprüfung, ob das Dokument einen Chip gemäß Prüfdefinitionen enthält		

MRZ = Machine Readable Zone = MLZ = „maschinenlesbarer Bereich“

Stand: Juni 2017