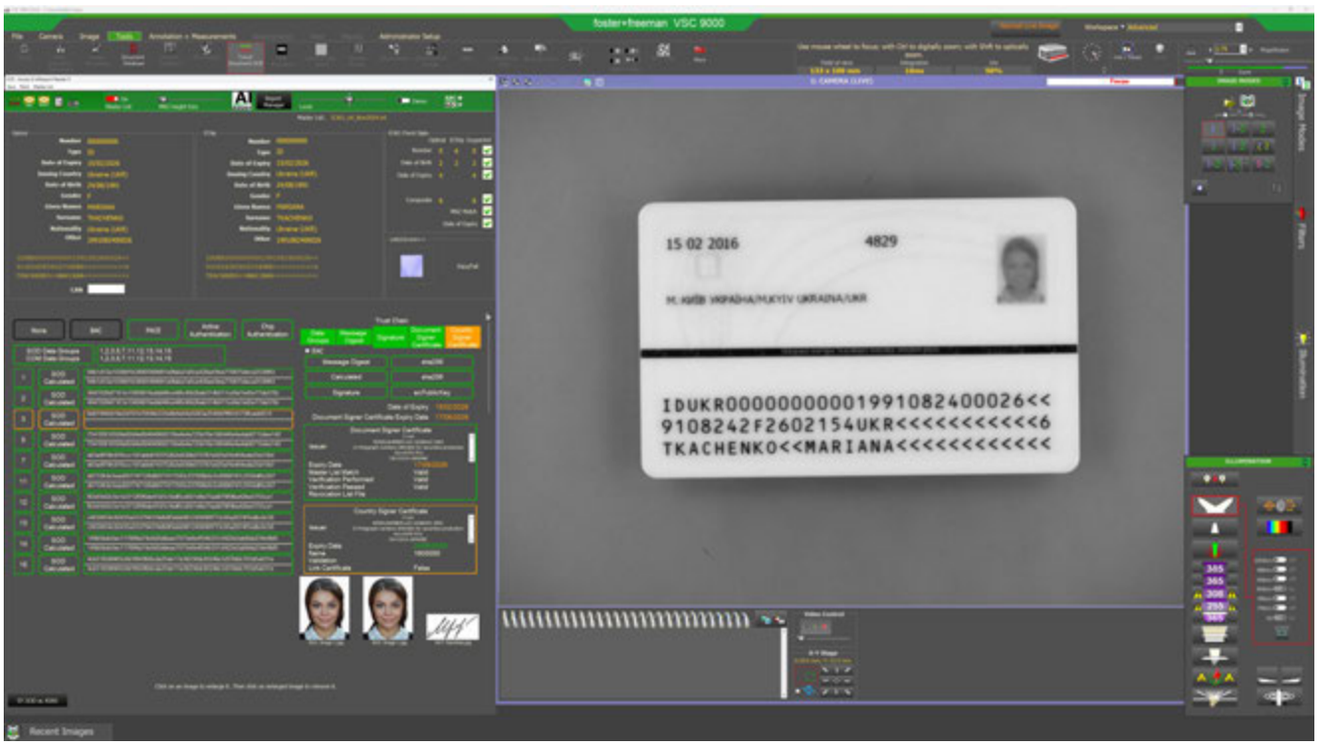
VSC STAC

Secure Trust Authentication Chain (Secure Trust-Authentifizierungskette)

Benutzerhandbuch für VSC Suite-Software



Die foster+freeman STAC-Software ermöglicht die Analyse von E-Chip-Daten mit einem außergewöhnlich hohen Detailgrad.

Handbuch-Version: 1.1
Letzte Aktualisierung: 02 Juni, 2026

Hauptgeschäftsstelle & UK Verkaufsbüro
foster+freeman Ltd
Vale Park
Evesham
Worcestershire
WR11 1TD
UK

+ 44 (0) 1386 768050
+ 44 (0) 1386 765351
sales@fosterfreeman.com
www.fosterfreeman.com

US-Verkaufsbüro
foster+freeman USA Inc
20145 Ashbrook Place
Ashburn
Virginia 20147
USA

+1 888 445 5048
+1 888 445 5049
usoffice@fosterfreeman.com
www.fosterfreeman.com

Deutsches Verkaufsbüro
foster+freeman Europe GmbH
Sandstr. 65
40878 Ratingen
Germany

+49 (2102) 557 6525
de.sales@fosterfreeman.com
www.fosterfreeman.com

Niederländisches Verkaufsbüro
foster+freeman Netherlands B. V.
Heerhugowaard
The Netherlands

+ 31 (0) 6 1114 38 58
nl.sales@fosterfreeman.com
www.fosterfreeman.com

Kundenbetreuung und Feedback
foster+freeman begrüßt Rückmeldungen von Kunden zu diesem Produkt. Bitte wenden Sie sich an eines unserer Büros, wenn Sie Ihre Kommentare weitergeben möchten.
foster+freeman bietet Beratung, Installation, Schulung und Vor-Ort-Wartung weltweit für alle ihre Produkte an.
customersupportteam@fosterfreeman.com

Spezifikation
foster+freeman behält sich das Recht vor, die Spezifikationen dieses Produkts, des Zubehörs und der Verbrauchsmaterialien ohne vorherige Ankündigung zu ändern.

Copyright

Sicherheitsmechanismen für eMRTDs

Es gibt mehrere Sicherheitsmechanismen für eMRTDs (electronic Machine Readable Travel Documents, elektronische maschinenlesbare Reisedokumente).

MRZ / CAN

Beim Zugriff auf E-Chip-Daten für Identitätsdokumente sind viele Elemente beteiligt. Der Hauptzugriff erfolgt entweder über eine maschinenlesbare Zone (MRZ, Machine-Readable Zone) oder über eine Kartenzugangsnummer (CAN, Card Access Number). MRZs können sich entweder am unteren Rand eines Dokuments (TD3) oder auf der Rückseite eines Dokuments (TD1) befinden. MRZs können entweder aus zwei Datenzeilen bei einem Dokument im TD3-Format oder aus drei Datenzeilen bei einem Dokument im TD1-Format bestehen. Die CAN ist ein 6-stelliger Code oder ein Barcode, der in der Regel auf der Vorderseite einiger Arten von ID-Dokumenten aufgedruckt ist. Die CAN kann nur mit PACE verwendet werden.

BAC / PACE

BAC (Basic Access Control, Einfache Zugangskontrolle) und PACE (Password Authenticated Connection Establishment, Passwort authentisierter Verbindungsaufbau) sind Zugangskontrollprotokolle, deren Zweck es ist, die auf dem eMRTD gespeicherten Daten vor Skimming zu schützen. Sobald der Zugang gewährt wird, können Daten vom E-Chip gelesen werden.

BAC verwendet symmetrische Kryptographie, die denselben Schlüssel für sowohl Verschlüsselung als auch Entschlüsselung benutzt.

PACE ist eine Verbesserung von BAC, da hier asymmetrische Kryptographie (mit unterschiedlichen Schlüsseln für Verschlüsselung und Entschlüsselung) zum Einsatz kommt. PACE ist somit sicherer als die symmetrische Kryptographie.

Datengruppen

Ein E-Chip kann viele Datengruppen enthalten, die spezifische Informationen umfassen. Diese Informationen werden entweder zur Sicherheit oder zum Speichern von Informationen über das Dokument oder den Inhaber verwendet.

Es gibt bis zu 16 spezifische Datengruppen (DG#). Einige dieser Datengruppen sind für den zukünftigen Gebrauch reserviert, und einige werden unter Umständen nicht in jedem Dokument verwendet.

Die Datengruppen sind typischerweise im folgenden Format organisiert:

DG1 – MRZ-Information
DG2 – Gesichtsbild
DG3 – Fingerabdruck/-abdrücke
DG4 – Iris
DG5 – Sekundäres Bild
DG6 – Reserviert für zukünftigen Gebrauch
DG7 – Unterschrift
DG8 – Datenmerkmal(e)
DG9 – Strukturmerkmal(e)
DG10 – Substanzmerkmal(e)
DG11 – Zusätzliche personenbezogene Details
DG12 – Zusätzliche Dokument-Details
DG13 – Optionale Details
DG14 – Sicherheitsoptionen *
DG15 – Public-Key-Info
DG16 – Zu benachrichtigende Person(en)

Siehe ICAO: 9303 für weitere Informationen.

*DG14 wird zur Chip-Authentifizierung (CA) verwendet, aber die Tatsache, dass DG14 vorhanden ist, heißt nicht automatisch, dass eine CA durchgeführt werden kann. Die Datei kann auch Informationen enthalten, die in bestimmten Arten der aktiven Authentifizierung (ECDH-Key-Vereinbarung) verwendet werden, und Informationen für die Durchführung von PACE wiederholen.

Zusätzlich zu den Datengruppen werden andere Dateien auf dem Chip gespeichert, z. B.:

- **SOD-Datei (Security Object of the Document, Sicherheitsobjekt des Dokuments)**
  - Umreißt, welche Datengruppen auf dem Chip gespeichert sind.
  - Speichert die einzigartigen Hash-Werte für jede Datengruppe.

- **COM-Datei (Common)**
  - Listet die Datengruppen auf, die vorhanden sind.
  - *Diese Information ist nicht digital signiert.*

Hashes

Durch das Hashing der Daten wird eine Zeichenkette mit einer festen Länge erstellt, die als einzigartige Kennung für die Originaldaten fungiert. Wenn ein Wert oder wenn die Originaldaten geändert werden, ist der resultierende Hash komplett anders. Die bereitgestellte Ausgabe ist im Hexadezimal-Format geschrieben.

Die Hashes für die Datengruppen werden mit Standard-Hash-Algorithmen wie z. B. sha-256 (hash = 32 Bytes /256 Bits) berechnet.

Hashes von allen Datengruppen werden in einer Hash-Tabelle in der SOD-Datei auf dem E-Chip gespeichert.

Ein Message Digest wird erstellt, indem die Hash-Tabelle gehasht wird, um ein „Komposit“-Hash bereitzustellen. „Digest“ ist ein anderes Wort für „Hash“.

Document Signer-Zertifikat

Die ausstellende Behörde erstellt ein Key-Paar:
- Einen Private-Key, der für die Verschlüsselung des Message-Digests (MD) verwendet wird, um eine digitale Signatur (SOD-Signatur) zu erstellen.
- Einen Public-Key, der für die Entschlüsselung der digitalen Signatur verwendet und der direkt auf dem Chip in der Zertifikatsdatei gespeichert wird.

Der Aussteller und das Subjekt eines Document Signer Zertifikats können nicht identisch sein.

Das Document Signer Zertifikat (DSC) enthält den Public-Key, der zur Verifizierung der SOD-Signatur verwendet wird.

Wurzelzertifikat

Die Wurzelzertifikat-Behörde (CSCA, Country Signing Certificates Authority) stellt selbstsignierte Wurzelzertifikate (Country Signing Certificates, CSCs) aus, die zur Verifizierung der Authentizität des DCS verwendet werden können, um die legitime Ausstellung des Zertifikats durch die Behörde des Landes zu bestätigen.

CSCA-Zertifikate können als individuelle Zertifikate oder in einer Liste kompiliert bereitgestellt werden, die als „Masterliste“ bezeichnet wird.

CSCAs können über das ICAO Public Key Directory (PKD) verteilt werden, um es einem Land zu ermöglichen, Daten auf E-Chips von anderen Ländern zu authentifizieren.

CSCAs können individuelle Zertifikate oder in einer signierten „Masterliste“ kompiliert sein. Masterlisten (ML) müssen innerhalb der STAC-Software verifiziert werden. Dies kann durch Laden in das entsprechende CSCA-Zertifikat für die ML erfolgen. Hierdurch wird verifiziert, dass die ML vom Signierer der Masterliste signiert wurde, der die Masterliste erstellt hat, und dass die ML vom CSCA-Zertifikat signiert wurde, der sie bereitgestellt hat, ähnlich wie die Verifizierung des DSC in der SOD.

Authentifizierungsmethoden

Es gibt mehrere Authentifizierungsmethoden.

Passive Authentifizierung

Passive Authentifizierung (PA, Passive Authentication) ist der Prozess, bei dem verifiziert wird, ob die Daten auf einem E-Chip geändert wurden, während gleichzeitig sichergestellt wird, dass die Daten von einer echten ausstellenden Behörde erhalten wurden.

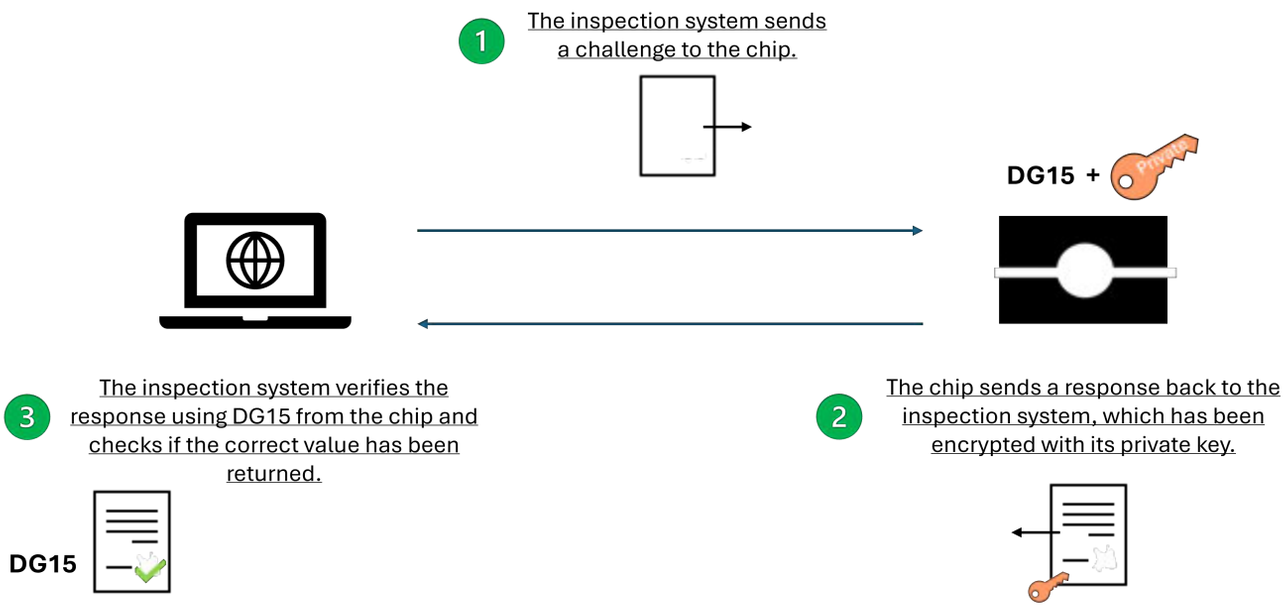
Die Verifizierung der Daten erfolgt durch eine erneute Berechnung des Hash-Wertes beim Lesen jeder Datengruppe und dem Vergleich der Ergebnisse mit den Hash-Werten, die zum Zeitpunkt der Personalisierung in der SOD-Datei gespeichert wurden. Ein anderer berechneter Hash impliziert, dass die Daten seit dem Zeitpunkt der Ausstellung verändert wurden.

Dieser Prozess des Vergleichs der Hash-Werte wird auch auf dem MD (dem Komposit-Hash) gegen den erneut berechneten Hash der SOD-Hash-Tabelle durchgeführt. Wenn in der SOD gespeicherte Hash-Werte verändert wurden (um z. B. einer veränderten DG-Datei zu entsprechen), stimmen die neu berechneten Komposit-Hash-Werte der SOD-Hash-Tabelle beim Vergleich nicht mit dem MD überein.

Um zu bestätigen, dass die Chip-Daten von einer echten ausstellenden Behörde bereitgestellt wurden, wird der DSC-Public-Key zur Entschlüsselung der SOD-Signatur verwendet und das ursprüngliche MD bereitgestellt, das dem neu berechneten MD entspricht. Die ML oder das vertraute CSC kann dann verwendet werden, um zu verifizieren, dass das DSC von der korrekten CSCA ausgestellt wurde.

Aktive Authentifizierung (optional)

Aktive Authentifizierung (AA, Active Authentication) ist ein Klonerkennungsprotokoll. Das Inspektionssystem sendet eine Challenge an den Chip, der digital vom Private-Key signiert ist, der innerhalb des E-Chips gespeichert ist. Das Inspektionssystem kann dann den Public-Key des Chips innerhalb von DG15 verwenden, um die Antwort zu verifizieren.



Chip-Authentifizierung

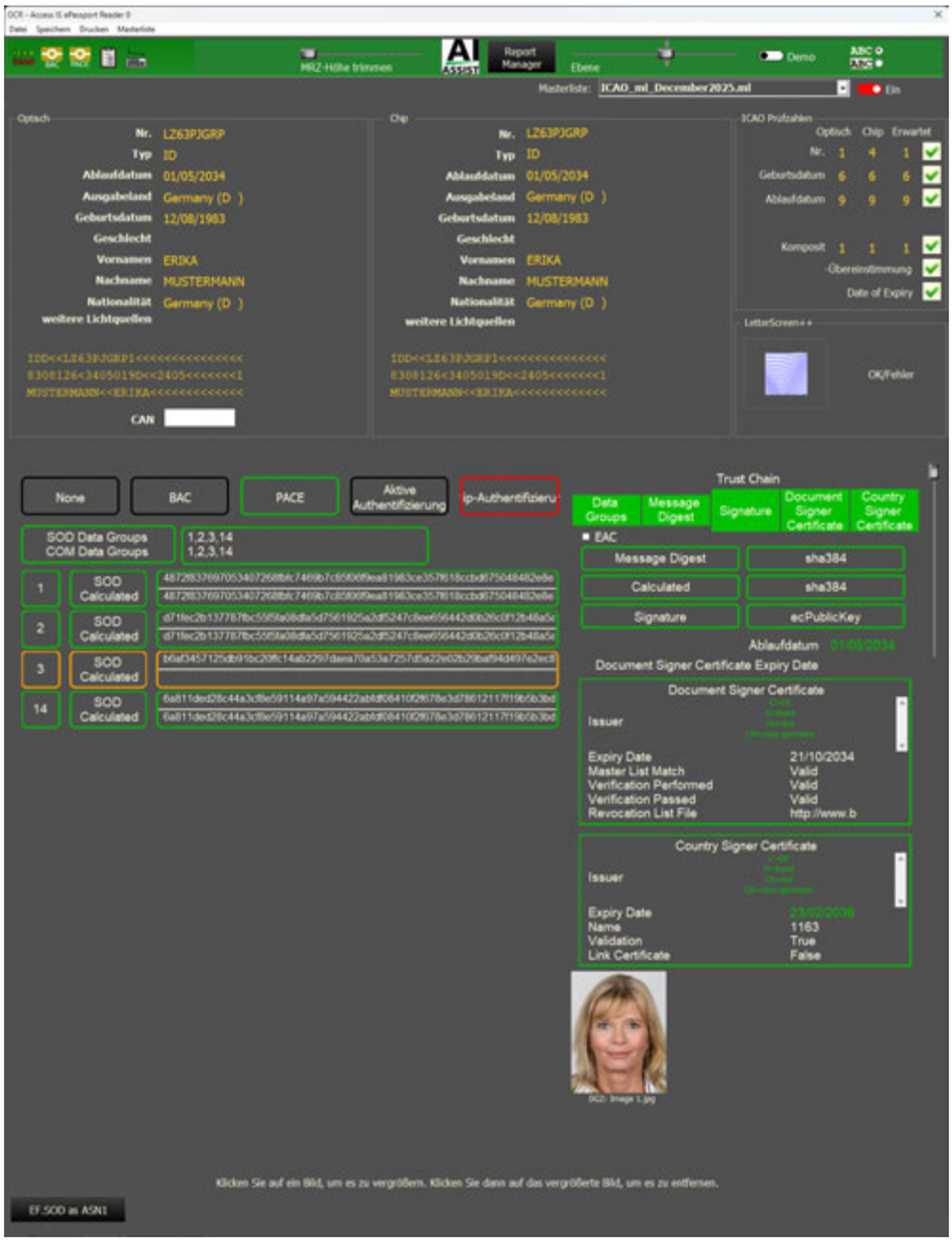
Chip-Authentifizierung (CA, Chip Authentication) ist eine Methode zur Klonerkennung, die einen sicheren Nachrichtenkanal zwischen dem Leser und dem E-Chip mittels des Diffie-Hellman-Key-Austauschmechanismus erstellt. CA ist erforderlich, wenn DG3 und DG4 gelesen werden müssen; ansonsten wird CA zur Verifizierung verwendet, ob der Chip original und kein Klon ist.

Erweiterte Zugangskontrolle

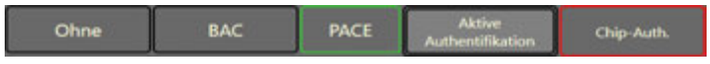
Erweiterte Zugangskontrolle (EAC, Extended Access Control) ist eine Sicherheitsmaßnahme, deren Zweck es ist, die vertraulichen biometrischen Daten zu schützen, die typischerweise in Datengruppe 3 und 4 (Fingerabdruck- und Iris-Scans) gespeichert sind. Um Zugang zu diesen Daten zu erhalten, ist ein Prozess zur Verifizierung der Befugnis des Terminals notwendig, um zu gewährleisten, dass der Zugang nur Personen mit entsprechender Berechtigung gewährt wird. Sind diese Zertifikate nicht in der Software installiert, können die Hash-Werte der geschützten Dateien, DG3 und DG4, folglich nicht für passive Authentifizierung berechnet werden. Information regarding the required certificate chain can be found in the EF. CVCA. Diese Kette besteht aus mehreren Zertifikaten.

Software-Funktionen

E-Chip-Bildschirm

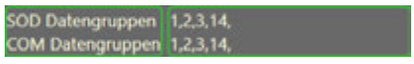


BAC / PACE / Keine / Aktive Authentifizierung / Chip-Authentifizierung



Angabe, welche Sicherheitsprotokolle auf dem E-Chip durchgeführt wurden.
Dies ist von Dokument zu Dokument unterschiedlich, da die jeweiligen Funktionen variieren.

Vergleich von SOD- und COM-Dateien



Dies zeigt, welche Datengruppen in der SOD- und der COM-Datei aufgelistet sind. Diese sollten übereinstimmen.
Eine Nichtübereinstimmung könnte darauf hinweisen, dass Datengruppen versteckt sind, um ein Lesen zu verhindern.

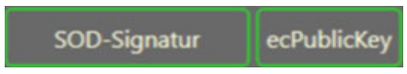
Berechnete ggü. gespeicherten Hash-Werten

Die berechneten Hash-Werte sollten mit den in der SOD-Datei gespeicherten Hash-Werten übereinstimmen.
Eine Nichtübereinstimmung könnte darauf hinweisen, dass Informationen verändert wurden, seit das Dokument ausgestellt wurde.

Message-Digest

Die berechneten Hash-Werte sollten mit den in der SOD-Datei gespeicherten Hash-Werten übereinstimmen.
Eine Nichtübereinstimmung könnte darauf hinweisen, dass Informationen verändert wurden, seit das Dokument ausgestellt wurde.

SOD-Signatur



Dies ist eine digitale Signatur, die durch digitales Signieren der Daten mithilfe des Private-Keys des Document Signer Zertifikats erstellt wurde.

SHA-Anzeige

Die Software ermittelt automatisch den korrekten Hash-Algorithmus, der verwendet werden muss. Verschiedene Hash-Algorithmen haben unterschiedlich lange Zeichenketten. Der verwendete SHA-Algorithmus wird angezeigt.

Vertrauenskette

Die Vertrauenskette wird verwendet, um schnell Fehler zu identifizieren, die die STAC-Software innerhalb der E-Chip-Daten identifiziert hat.

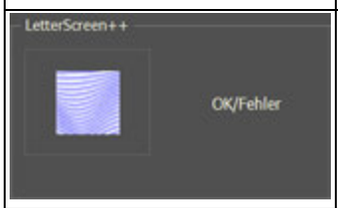
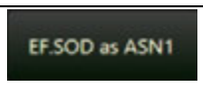
Jeder Abschnitt des Vertrauensketten-Überblicks gibt mithilfe der folgenden Farben einen Vertrauensgrad an.

Grün	Keine Fehler entdeckt.
Gelb	Weitere Inspektion erforderlich.
Rot	Fehler entdeckt.

Abschnitte im Vertrauensketten-Überblick:

Datengruppen	Verifizierung, dass die neu berechneten Hash-Werte mit denen übereinstimmen, die in der SOD-Datei auf dem Chip gespeichert sind.
Message-Digest	Verifizierung, dass der neu berechnete Hash der SOD-Hash-Tabelle mit dem MD innerhalb der SOD übereinstimmt.
SOD-Signatur	Verifizierung der erfolgreichen Entschlüsselung der SOD-Signatur mit dem DSC, und das Ergebnis stimmt mit dem erwarteten Ergebnis überein.
Document Signer-Zertifikat	Verifizierung des DSC mithilfe des zugehörigen CSC.
Wurzelzertifikat	Verifizierung, dass das CSC von einer vertrauenswürdigen Quelle erhalten wurde.

Andere Steuerelemente:

	**EAC-Kontrollkästchen**	Dieses Kontrollkästchen aktivieren, um die Ergebnisse von Datengruppe DG3 und DG4 in den Vertrauensketten-Überblick einzuschließen. Diese sind normalerweise unter weiteren Sicherheitsmaßnahmen (Terminal-Authentifizierung) geschützt. Dieses Kontrollkästchen ist aufgrund der Forderung zusätzlicher Zertifikate, diese Daten gründlich zu untersuchen, standardmäßig deaktiviert, was bedeutet, dass DG3 und DG4 ignoriert werden.
	**LetterScreen++**	(Wenn lizenziert) Auswählen, um den LS++-Bildschirm zu öffnen und ein LS++-Muster zu verifizieren.
	**EF.SOD as ASN1**	Auswählen, um die EF.SOD-Datei im Format ASN1 anzuzeigen.

Hinweis: Die in der STAC-Software verwendeten Verfahren entsprechen den Richtlinien, die im ICAO-Dokument 9303 aufgelistet sind. Dokumente, die nicht den ICAO-Empfehlungen entsprechen, unabhängig von ihrer Authenzität, werden unter Umständen in der Software geflaggt.

Masterliste

CSCs können individuelle Zertifikate oder in einer Liste kompiliert sein, die als „Masterliste“ bezeichnet wird. CSCs können zur Verifizierung der Authenzität des DSC verwendet werden. Dies bestätigt, ob das

DSC legitim von der Behörde des Landes ausgestellt wurde.

Die Masterliste über das Dropdown-Menü in der Titelleiste des OCR-Fensters laden.

Die Masterliste aktivieren, bevor ein E-Chip gelesen wird.

Glossar der Akronyme

AA	Aktive Authentifizierung
BAC	Basic Access Control (Einfache Zugangskontrolle)
CA	Chip-Authentifizierung
CAN	Card Access Number (Kartenzugangsnummer)
COM	Common
CSC	Wurzelzertifikat
CSCA	Country Signing Certificate Authority (Wurzelzertifikat-Behörde)
DG#	Nummer der Datengruppe
DSC	Document Signer-Zertifikat
EAC	Erweiterte Zugangskontrolle
eMTRD	Electronic Machine Readable Travel Document (Elektronisches maschinenlesbares Reisedokument)
ICAO	International Civil Aviation Organisation (Internationale Zivilluftfahrtorganisation)
ML	Masterliste, ein ICAO-spezifischer signierter CSCA-Container in einem bestimmten Format.
MRZ	Machine Readable Zone (Maschinenlesbare Zone)
PA	Passive Authentifizierung
PACE	Password Authenticated Connection Establishment (Passwort authentisierter Verbindungsaufbau)
PKD	Public Key Directory (Public-Key-Verzeichnis)
STAC	Secure Trust Authentication Chain (Secure Trust-Authentifizierungskette)

foster+freeman

FORENSIC SCIENCE INNOVATION

Mit der foster+freeman Ltd. in Kontakt bleiben:

https://www.youtube.com/user/fosterfreeman

https://x.com/fosterfreeman

https://www.facebook.com/fosterandfreeman/

https://www.instagram.com/fosterfreemanforensics/

https://uk.linkedin.com/company/foster-freeman