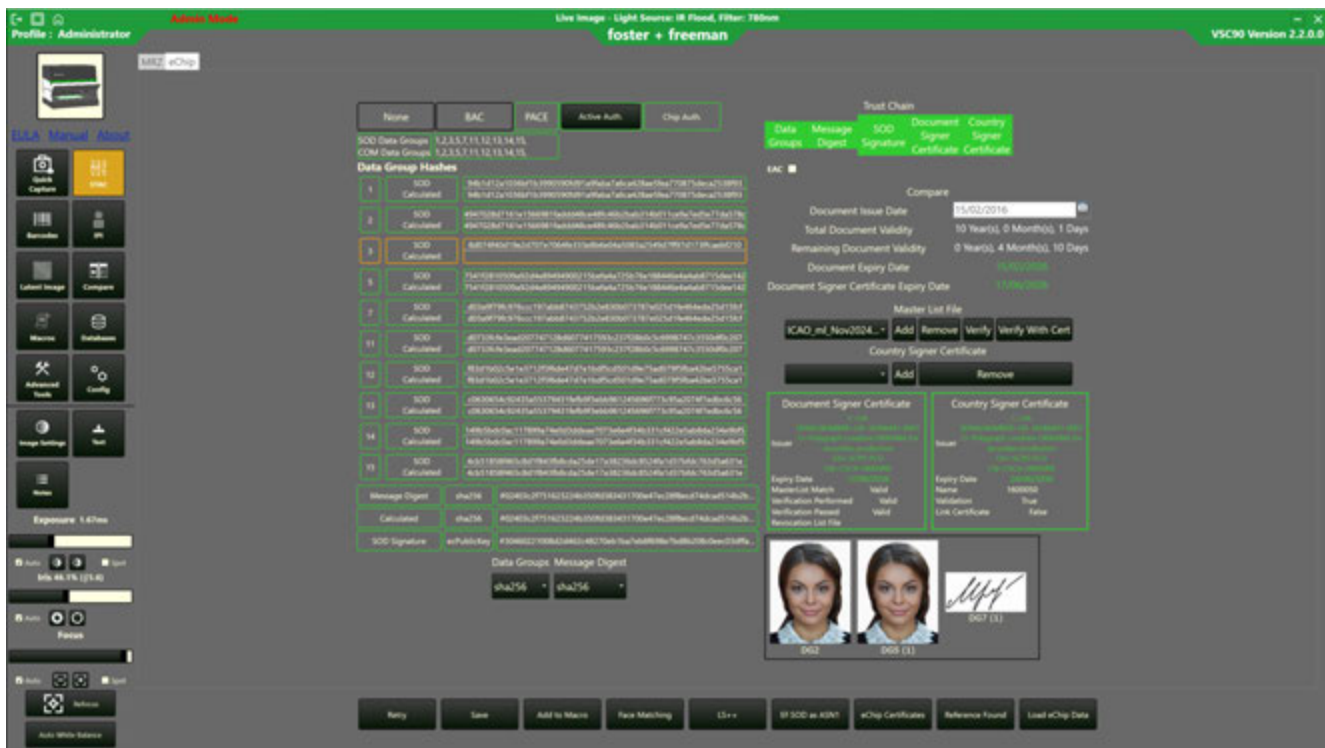


# VSC STAC

## Secure Trust Authentication Chain User Guide for VSCi Software



The foster+freeman STAC software allows for the analysis of e-Chip data to an exceptional level of detail.

Revision: 1.1  
Last Updated: 17 February, 2026  
Copyright © foster+freeman Ltd

## Head Office & UK Sales Office

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

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

## German Sales Office

foster+freeman Europe GmbH  
Sandstr. 65  
40878 Ratingen  
Germany

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

## US Sales Office

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

## Dutch Sales Office

foster+freeman Netherlands B.V.  
Heerhugowaard  
The Netherlands

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

## Customer Support and Feedback

foster+freeman welcome feedback from Customers regarding this product. Please contact one of our offices if you would like to pass on your comments.

foster+freeman are pleased to offer advice, installation, training and on-site maintenance worldwide for all of their products.

✉ customersupportteam@fosterfreeman.com

## Specification

foster+freeman reserves the right to alter the specification of this product, accessories, and consumables without prior notice.

## Copyright

This document contains proprietary information that is protected by copyright.

All rights are reserved. No part of this publication may be reproduced in any form whatsoever without prior, written permission of foster+freeman Ltd.

Copyright © foster+freeman Ltd

<b>Security Mechanisms for eMRTDs</b> .....	<b>4</b>
MRZ / CAN .....	4
BAC / PACE .....	4
Data Groups .....	4
Hashes .....	5
Document Signer Certificate .....	5
Country Signing Certificate .....	5
Authentication Methods .....	5
Passive Authentication .....	5
Active Authentication (Optional) .....	6
Chip Authentication .....	6
Extended Access Control .....	6
<b>Software Functions</b> .....	<b>7</b>
e-Chip Screen .....	7
BAC / PACE / None / Active Authentication / Chip Authentication .....	7
Comparison of SOD and COM Files .....	7
Calculated vs Stored Hash Values .....	8
Message Digest .....	8
SOD Signature .....	8
SHA Selection .....	8
Trust Chain .....	9
Master List .....	10
<b>Glossary of Acronyms</b> .....	<b>12</b>

# Security Mechanisms for eMRTDs

There are multiple security mechanisms for eMRTDs (electronic Machine Readable Travel Documents).

## MRZ / CAN

There are many elements involved in accessing e-Chip data for identity documents. The main access is either via Machine Readable Zone (MRZ) or Card Access Number (CAN). MRZs can be located either at the bottom of a document (TD3) or located on the back (TD1). MRZs can either be two or three lines of data for a TD3 and TD1 sized document respectively. CAN is a 6-digit code or barcode generally printed on the front of some types of ID documents. The CAN can only be used with PACE.

## BAC / PACE

Basic Access Control (BAC) and Password Authenticated Connection Establishment (PACE) are access control protocols that are in place to protect data stored on the eMRTD from skimming, and once access is granted, it is possible to read information from the e-Chip.

BAC uses symmetric cryptography which uses the same key for both encryption and decryption.

PACE is an improvement on BAC through the use of asymmetric cryptography (using different keys for encryption and decryption) which is more secure than symmetric cryptography.

## Data Groups

An e-Chip can contain many groups of data comprising of specific information, either used for security or to store information about the document or holder.

There are up to 16 dedicated Data Groups (DG#). Some of these Data Groups are reserved for future use, and some may not be utilised in every document.

They are typically organised in the following format:

DG1 – MRZ information	DG9 – Structure feature(s)
DG2 – Face image	DG10 – Substance feature(s)
DG3 – Fingerprint(s)	DG11 – Additional personal details
DG4 – Iris(es)	DG12 – Additional document details
DG5 – Secondary image	DG13 – Optional details
DG6 – Reserved for future use	DG14 – Security options *
DG7 – Signature	DG15 – Public key info
DG8 – Data feature(s)	DG16 – Person(s) to notify

*Refer to ICAO: 9303 for further information.*

\*While DG14 is used for chip authentication(CA), its presence is not indicative of it being possible to perform CA. The file can also contain information used in certain types of Active Authentication (ECDH key agreement), and a repeat of information for performing PACE.

In addition to the Data Groups, other files are stored on the chip, such as:

- **SOD file (Security Object of the Document)**
  - Outlines which Data Groups are stored on the chip.

- Stores the unique hash values for each Data Group.
- **COM file (Common)**
  - Lists the Data Groups that are present.
  - *This information is not digitally signed.*

## Hashes

Hashing the data creates a fixed-size string of characters that acts as a unique identifier for the original data. If one value or the original data is changed, the resulting hash is completely different. The output provided is written in hexadecimal.

The hashes for the Data Groups are calculated using standard hash algorithms, such as sha-256 (hash = 32 bytes / 256 bits).

Hashes from all Data Groups are stored in a hash table in the SOD file on the e-Chip.

A Message Digest is created by hashing the hash table to provide a 'composite' hash. A 'digest' is another term for a hash.

## Document Signer Certificate

The issuing authority creates a key-pair:

- A private key used for the encryption of the Message Digest (MD) to create a digital signature (SOD Signature)
- A public key used for the decryption of the digital signature, stored on the chip itself within the certificate file.

The Issuer and Subject of a document signer certificate cannot be exactly the same.

The Document Signer Certificate (DSC) contains the public key used to verify the SOD signature.

## Country Signing Certificate

Country Signing Certificates Authority (CSCA) issues self-signed root certificates (Country Signing Certificates, or CSCs) which can be used to verify the authenticity of the DSC to confirm it was a legitimate issue by the country's authority.

CSCA certificates can be provided as individual certificates or compiled into a list known as a 'MasterList'.

CSCAs can be distributed via the ICAO Public Key Directory (PKD) to allow a country to authenticate data on e-Chips from other countries.

CSCAs can be individual certificates or compiled into a signed 'MasterList'. MasterLists (ML) need verifying within the STAC software. This can be done by loading in the appropriate CSCA certificate for the ML. Doing this will verify that the ML was signed by the MasterList Signer created and signed by the CSCA certificate provided, much like the verifying the DSC in the SOD.

## Authentication Methods

There are multiple authentication methods.

### Passive Authentication

Passive Authentication (PA) is the process of verifying if the data on an e-Chip has been changed, whilst ensuring it has been obtained from a genuine issuing authority.

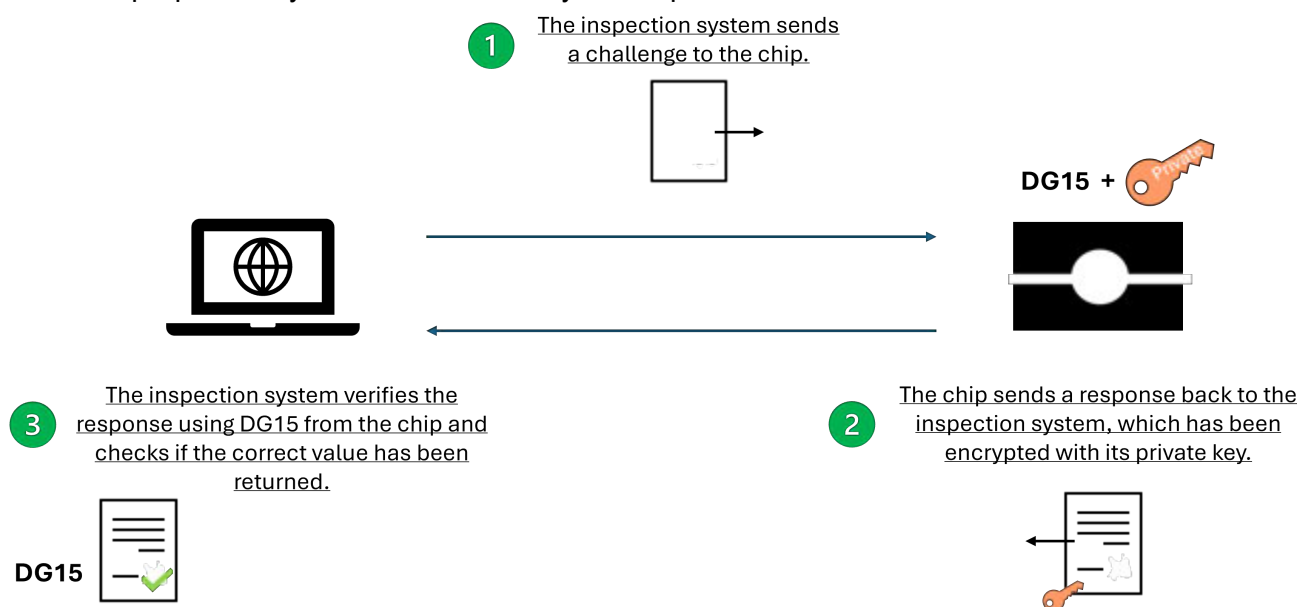
Verification of the data is achieved by re-calculating the hash value on reading each Data Group and comparing the results with the hash values stored in the SOD file at the point of personalisation. A different calculated hash implies that the data has been altered since the time of issue.

This process of comparing the hashes is also carried out on the MD (the composite hash) against the re-calculated hash of the SOD hash table. If hash values stored in the SOD have been altered (such as to match an altered DG file), the re-calculated composite hash values of the SOD hash table will not match the MD when compared.

To confirm that the chip data has been provided by a genuine issuing authority, the DSC public key is used to decrypt the SOD signature, providing the original MD which will match the re-calculated MD. The ML or trusted CSC can then be used to verify the DSC has been issued by the correct CSCA.

### Active Authentication (Optional)

Active Authentication (AA) is a clone detection protocol. The inspection system sends a challenge to the chip which is digitally signed by the private key stored within the e-Chip. The inspection system can then use the chip's public key within DG15 to verify the response.



### Chip Authentication

Chip authentication (CA) is a method of clone detection which creates a secure messaging channel between the reader and the e-Chip using the Diffie-Hellman key exchange mechanism. CA is required if DG3 and DG4 are to be read, otherwise it is used to verify that the chip is original and not a clone.

### Extended Access Control

Extended Access Control (EAC) is a security measure in place to protect the sensitive biometric data that is typically stored in Data Group 3 and 4 (fingerprint and iris scans). To access this data, a process of verifying the authority of the terminal is needed to ensure that access is only given to those with permission. As a result, if these certificates are not installed in the software, the hash values of the protected files, DG3 and DG4, cannot be calculated for Passive Authentication. Information regarding the required certificate chain can be found in the EF.CVCA. This chain consists of multiple certificates.

# Software Functions

## e-Chip Screen

The screenshot displays the 'e-Chip Screen' interface with the following sections:

- Authentication Options:** None, BAC, PACE, Active Auth. (selected), Chip Auth.
- Data Groups:** SOD Data Groups: 1,2,3,5,7,11,12,13,14,15; COM Data Groups: 1,2,3,5,7,11,12,13,14,15.
- Data Group Hashes:** A list of 15 rows showing SOD Calculated hashes for various data groups (1, 2, 3, 5, 7, 11, 12, 13, 14, 15).
- Trust Chain:**
  - Data Groups: SOD Signature
  - Message Digest: Document Signer Certificate
  - Country Signer: Country Signer Certificate
- Compare:**
  - Document Issue Date: 15/02/2016
  - Total Document Validity: 10 Year(s), 0 Month(s), 1 Days
  - Remaining Document Validity: 0 Year(s), 4 Month(s), 10 Days
  - Document Expiry Date: 15/02/2026
  - Document Signer Certificate Expiry Date: 17/06/2026
- Master List File:** ICAO\_ml\_Nov2024... with buttons for Add, Remove, Verify, and Verify With Cert.
- Certificate Verification:**
  - Document Signer Certificate:** Issuer: POLYGRAPH LITHUANIA, Expiry Date: 17/06/2026, Verification Status: Valid.
  - Country Signer Certificate:** Issuer: POLYGRAPH LITHUANIA, Expiry Date: 24/06/2030, Verification Status: True.
- Visuals:** Two portrait photos labeled DG2 and DGS (1), and a signature labeled DG7 (1).
- Buttons:** Retry, Save, Add to Macro, Face Matching, LS++, EF.SOD as ASN1, eChip Certificates, Reference Found, Load eChip Data.

### BAC / PACE / None / Active Authentication / Chip Authentication



Indication of what security protocols have been carried out on the e-Chip. This will differ between documents as their capabilities vary.

### Comparison of SOD and COM Files

SOD Data Groups: 1,2,3,5,7,11,12,13,14,15  
 COM Data Groups: 1,2,3,5,7,11,12,13,14,15

This shows what Data Groups are listed in the SOD and COM file. These should match. A mismatch could indicate that Data Groups are being hidden to prevent reading.

## Calculated vs Stored Hash Values

Data Group Hashes		
1	SOD Calculated	94b1d12a1036bf1b3990590fd91a9faba7a6ca428ae5fea770875deca2538f93 94b1d12a1036bf1b3990590fd91a9faba7a6ca428ae5fea770875deca2538f93
2	SOD Calculated	4947028d7161e1566981fadd48ce48fc46b2bab314b011ce9a7ed5e77da578c 4947028d7161e1566981fadd48ce48fc46b2bab314b011ce9a7ed5e77da578c
3	SOD Calculated	8d074f40d19e2d707e7064fe333e8b6e04a5083a2549d7ff97d173ffcaebf210 
5	SOD Calculated	7541f2810509a92d4e89494900215befa4a725b76e188446e4a4ab8715dee142 7541f2810509a92d4e89494900215befa4a725b76e188446e4a4ab8715dee142
7	SOD Calculated	d03a9f79fc976ccc197abb8743752b2e830b073787e025d1fe464ede25d15fcf d03a9f79fc976ccc197abb8743752b2e830b073787e025d1fe464ede25d15fcf
11	SOD Calculated	d0733fcfe3ead207747128d6077417593c237f28b0c5c6998747c3550df0c207 d0733fcfe3ead207747128d6077417593c237f28b0c5c6998747c3550df0c207
12	SOD Calculated	f83d1b02c5e1e3712f5f6de47d7e1bdf5cd501d9e75ad079f5fba42be5755ca1 f83d1b02c5e1e3712f5f6de47d7e1bdf5cd501d9e75ad079f5fba42be5755ca1
13	SOD Calculated	c0630654c92435a55379431fefb9f3ebb961245696f773c95a2074f7edbc6c56 c0630654c92435a55379431fefb9f3ebb961245696f773c95a2074f7edbc6c56
14	SOD Calculated	149b5bdc0ac117899a74e0d3ddeae7073e6e4f34b331cf422e5ab8da234e9bf5 149b5bdc0ac117899a74e0d3ddeae7073e6e4f34b331cf422e5ab8da234e9bf5
15	SOD Calculated	4cb51858f465c8d1f843fb8cda25de17a38236dc8524fa1d37bfdc763d5a631e 4cb51858f465c8d1f843fb8cda25de17a38236dc8524fa1d37bfdc763d5a631e

The calculated hashes should match those stored in the SOD file.  
A mismatch may indicate that information has been changed since the document was issued.

## Message Digest

Message Digest	sha256	#02403c2f751623224b350fd383431700e47ec28f8ecd74dcad514b2b...
Calculated	sha256	#02403c2f751623224b350fd383431700e47ec28f8ecd74dcad514b2b...

The calculated hashes should match those stored in the SOD file.  
A mismatch may indicate that information has been changed since the document was issued.

## SOD Signature

SOD Signature	ecPublicKey	#30460221008d2d462c48270eb1ba7eb8f698e7bd8b208c0eec03dffa...
---------------	-------------	--

This is a digital signature created by digitally signing the data using the private key of the Document Signer Certificate.

## SHA Selection

Data Groups	Message Digest
sha256	sha256

Changing the SHA-algorithm will alter the method of calculating the hash values. Different hash algorithms have varying lengths of character strings.  
The software will automatically determine the correct hash algorithm to use. Alternative methods can be selected if required.

## Trust Chain

Trust Chain				
Data	Message	SOD	Document	Country
Groups	Digest	Signature	Signer	Signer
			Certificate	Certificate

The Trust Chain is used to quickly identify errors that the STAC software has identified within the e-Chip data.




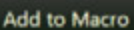

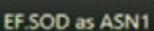
Each section of the Trust Chain summary will indicate a level of trust using the following colours:

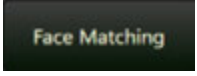
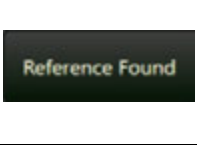
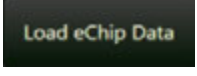
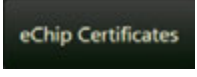
<b>Green</b>	No errors detected.
<b>Amber</b>	Further inspection required.
<b>Red</b>	Errors detected.

Trust Chain summary sections:

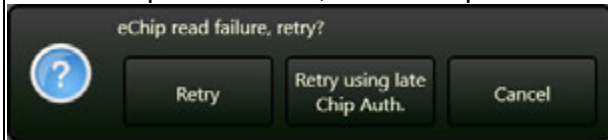
<b>Data Groups</b>	Verification that the calculated hash values align with those stored in the SOD file on the chip.
<b>Message Digest</b>	Verification that the re-calculated hash of the SOD hash table aligns with the MD within the SOD.
<b>SOD Signature</b>	Verification of the successful decryption of the SOD signature with the DSC, and the result matches the expected result (the original MD).
<b>Document Signer Certificate</b>	Verification of the DSC using the associated CSC.
<b>Country Signer Certificate</b>	Verification that the CSC has been obtained from a trustworthy source.

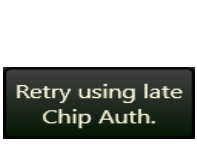
Other controls:

	<b>EAC tick box</b>	Select this tick box to allow for the inclusion of the results from Data Groups DG3 and DG4 in the Trust Chain summary. These are normally protected under further security measures (Terminal Authentication). By default, this is unticked due to the requirement of additional certificates to thoroughly investigate this data, meaning DG3 and DG4 are ignored.
	<b>Retry</b>	Select to retry e-Chip reading.
	<b>Save</b>	Select to save the e-Chip information, including MRZ and e-Chip images.
	<b>Save PDF</b>	Select to save the e-Chip data in either a non-editable PDF or an editable RTF file, using the desired report templates.
	<b>Save e-Chip Data</b>	Select to save all information as a .ff file.
	<b>Add to Macro</b>	Select to add e-Chip reading as a step to a selected macro sequence.
	<b>LetterScreen++</b>	If licensed, select to open the LS++ screen to verify an LS++ pattern.
	<b>EF.SOD as ASN1</b>	Select to display the EF.SOD file in ASN1 format.

	<b>Face Matching</b>	If licensed, select this to load the face image from the e-Chip to the Face Matching module for comparison.
	<b>Reference Found</b>	If licensed, this will open the correct document type and issuer in the document database for side-by-side comparison. There may be multiple results to navigate through depending on the relevant issue of the document.
	<b>Load e-Chip data</b>	Select to load pre-saved e-Chip data.
	<b>e-Chip Certificates</b>	Select to save the DSC or CSC.

If the e-Chip fails to read, then this option will become available:

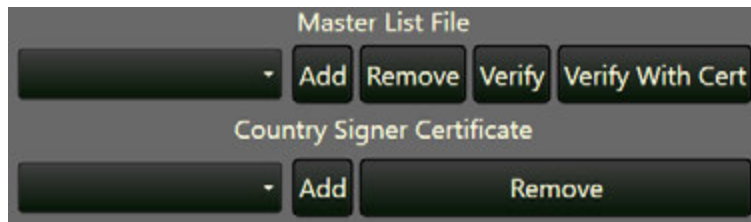


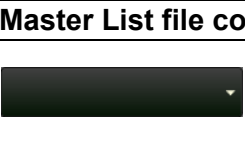
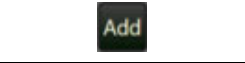
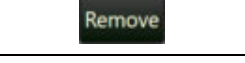

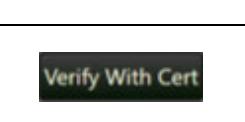
	<b>Retry using late Chip Auth.</b>	Chip authentication is a method of clone detection, but it also creates a secure messaging channel between the chip and the reader. ICAO guidelines state that this should be performed at the start of the process, which will cause false e-Chips to fail. Select this to perform chip authentication later in the process to allow for data collection before the channel fails.
---	------------------------------------	---

*Please note: The procedures used in the STAC software adhere to the guidelines listed in ICAO document 9303. Any documents that do not comply with ICAO recommendations, regardless of authenticity, may be flagged in the software.*

### Master List

CSCs can be individual certificates or compiled into a list known as a 'MasterList'. CSCs can be used to verify the authenticity of the DSC. This confirms if the DSC was legitimately issued by the country's issuing authority.



Master List file controls:		
	<b>Drop-Down Menu</b>	Select a specific MasterList or Country Signer Certificate from the drop-down menu.
	<b>Add</b>	Add MasterList or individual Country Signer Certificate.
	<b>Remove</b>	Remove MasterList or individual Country Signer Certificate.
	<b>Verify</b>	MasterLists need verifying within the STAC software. The first step of this process is to verify the signature of the MasterList using the MasterList signer certificate contained within the MasterList
	<b>Verify With Cert</b>	MasterLists need verifying within the STAC software. The second step is to verify the MasterList signer certificate with a separate certificate.



# Glossary of Acronyms

AA	Active Authentication
BAC	Basic Access Control
CA	Chip Authentication
CAN	Card Access Number
COM	Common
CSC	Country Signing Certificate
CSCA	Country Signing Certificate Authority
DG#	Data Group number
DSC	Document Signer Certificate
EAC	Extended Access Control
eMTRD	Electronic Machine Readable Travel Document
ICAO	International Civil Aviation Organisation
ML	MasterList, an ICAO-specific signed CSCA container of a particular format.
MRZ	Machine Readable Zone
PA	Passive Authentication
PACE	Password Authenticated Connection Establishment
PKD	Public Key Directory
STAC	Secure Trust Authentication Chain

# foster+freeman

## FORENSIC SCIENCE INNOVATION

Keep in touch with foster+freeman Ltd:



<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>