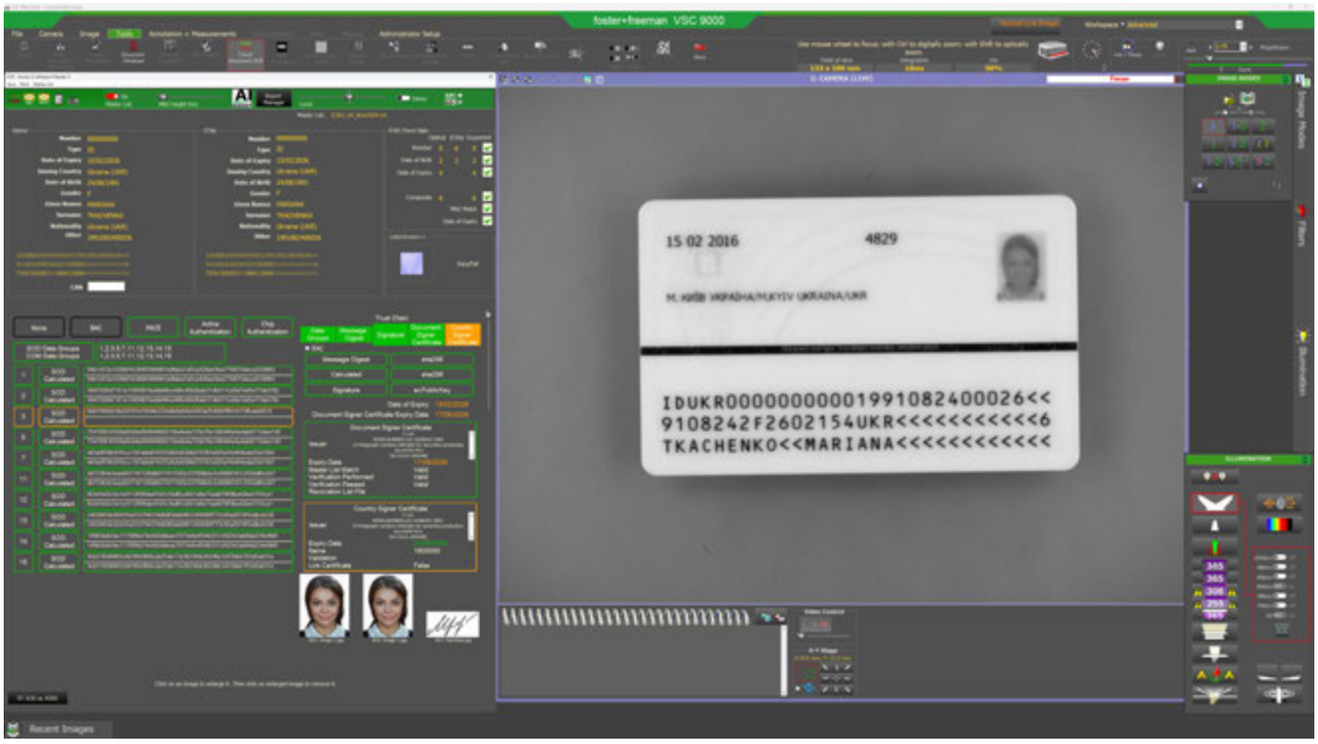
VSC STAC

Secure Trust Authentication Chain

User Guide for VSC Suite 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

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

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

German Sales Office
foster+freeman Europe GmbH
Sandstr. 65
40878 Ratingen
Germany

+49 (2102) 557 6525
de.sales@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

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

Refer to ICAO: 9303 for further information.

*While 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 tavle 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.

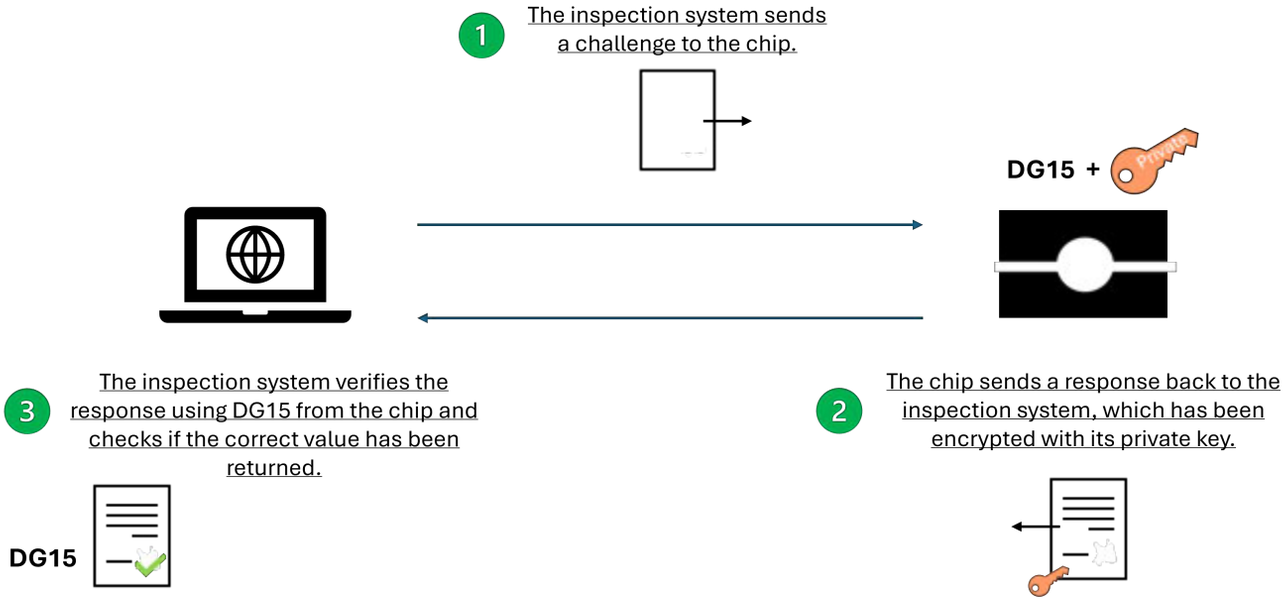
Verification of the data is achieved by re-calculating the hash value on reading each Data Group and comparing the results with the hash values stored in the SOD file at the point of personalisation. A different calculated hash implies that the data has been altered since the time of issue.

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

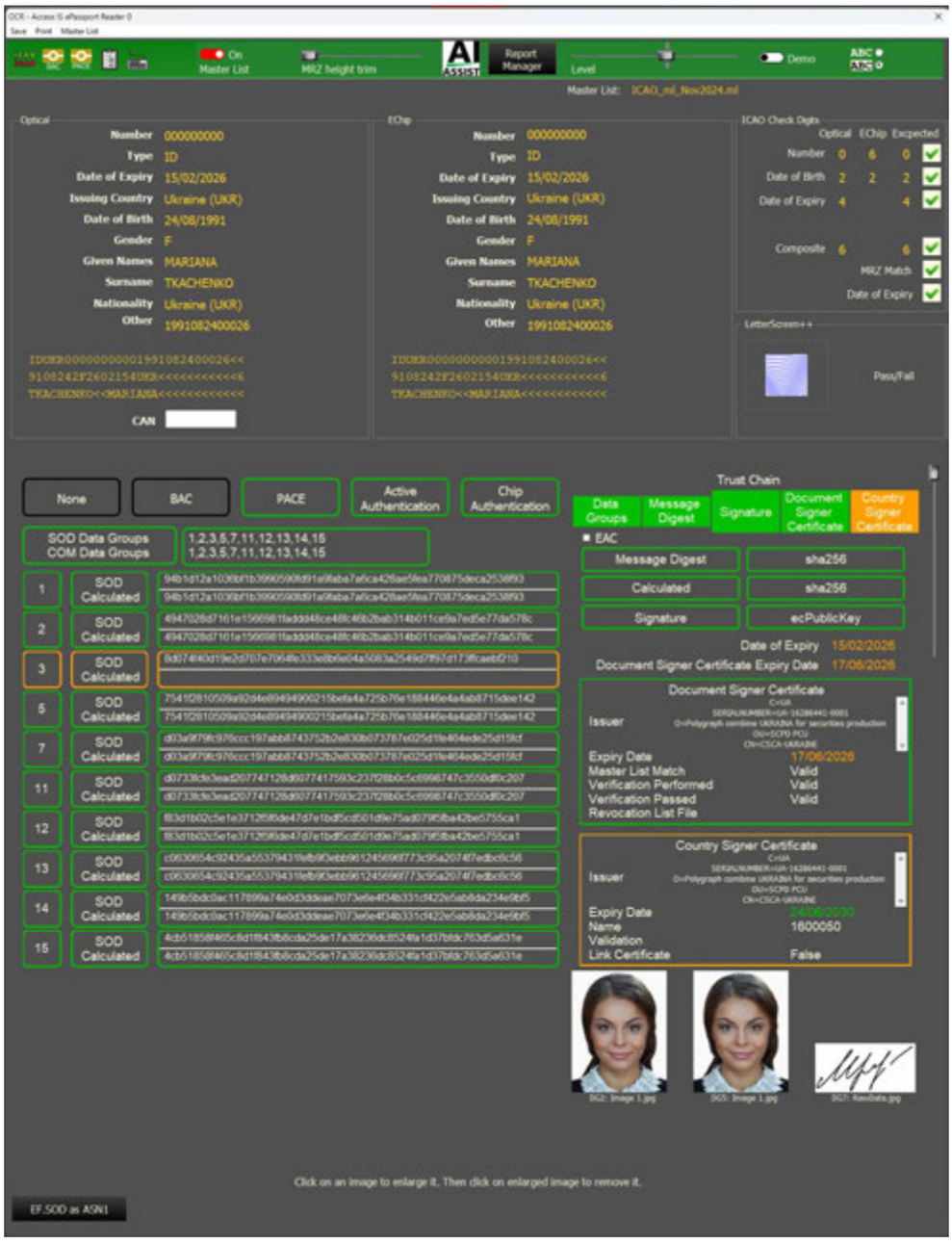
Chip authentication (CA) is a method of clone detection which creates a secure messaging channel between the reader and the e-Chip using the Diffie-Hellman key exchange mechanism. CA is required if DG3 and DG4 are to be read, otherwise it is used to verify that the chip is original and not a clone.

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

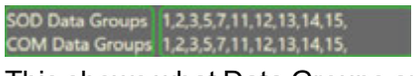
e-Chip Screen



BAC / PACE / None / Active Authentication / Chip Authentication

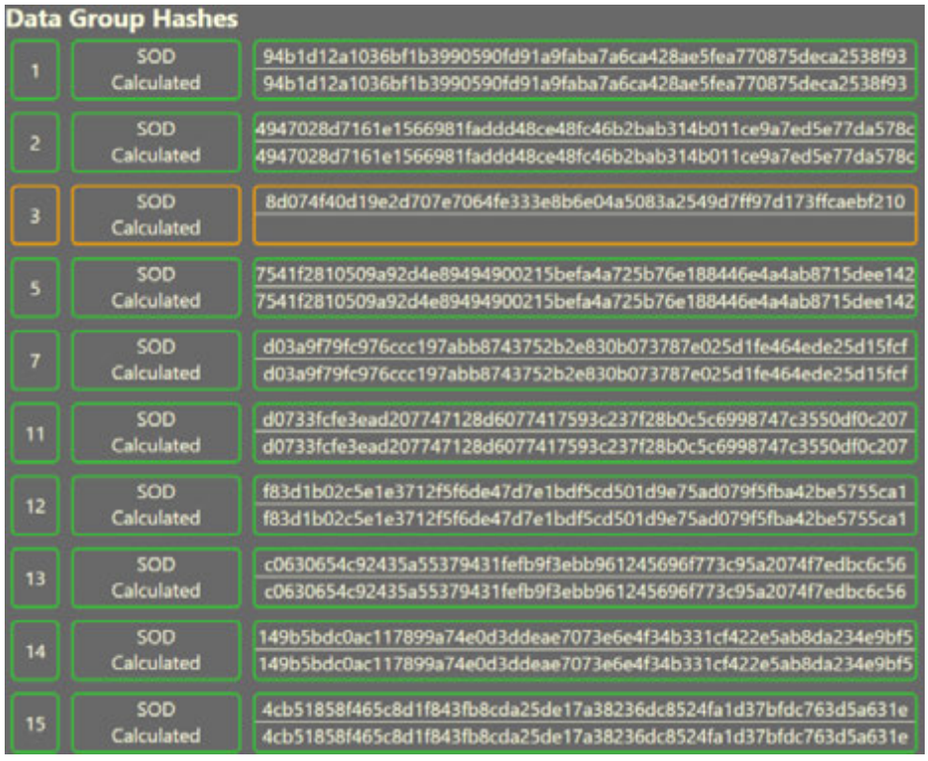
Indication of what security protocols have been carried out on the e-Chip.
This will differ between documents as their capabilities vary.

Comparison of SOD and COM Files



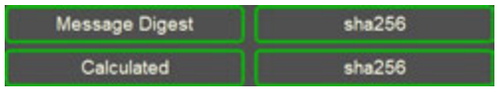
This shows what Data Groups are listed in the SOD and COM file. These should match.
A mismatch could indicate that Data Groups are being hidden to prevent reading.

Calculated vs Stored Hash Values



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



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

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

SHA Viewing

The software will automatically determine the correct hash algorithm to use. Different hash algorithms have varying lengths of character strings. The SHA-algorithm used will be displayed.

Trust Chain

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

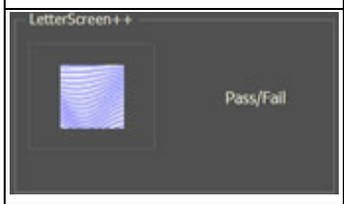
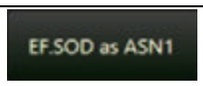
Each section of the Trust Chain summary will indicate a level of trust using the following colours:

Green	No errors detected.
Amber	Further inspection required.
Red	Errors detected.

Trust Chain summary sections:

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

Other controls:

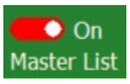
	**EAC tick box**	Select this tick box to allow for the inclusion of the results from Data Groups DG3 and DG4 in the Trust Chain summary. These are normally protected under further security measures (Terminal Authentication). By default, this is unticked due to the requirement of additional certificates to thoroughly investigate this data, meaning DG3 and DG4 are ignored.
	**LetterScreen++**	If licensed, select to open the LS++ screen to verify an LS++ pattern.
	**EF.SOD as ASN1**	Select to display the EF.SOD file in ASN1 format.

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 authority.

Load the MasterList via the drop-down menu in the title bar of the OCR panel.



Toggle "On" the Master List prior to reading an e-Chip.

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