Element Metech electronic calibration documents

Element Metech electronic calibration documents are published as PDF files and signed digitally. The documents are distributed by Metech Instrument Organizer, to registered users or as download links / attachments in delivery notification e-mails. You can also get the calibration documents from the Element Metech web site via the report number and MIO Id. If your calibration stickers have QR code, the calibration document can be opened directly in a mobile phone.

Element Metech digital signatures

Element Metech digital signatures replace the handwritten signatures in calibration documents (requirement ISO/IEC 17025:2017, 7.8.2.1 o - identification of the person(s) authorizing the report).

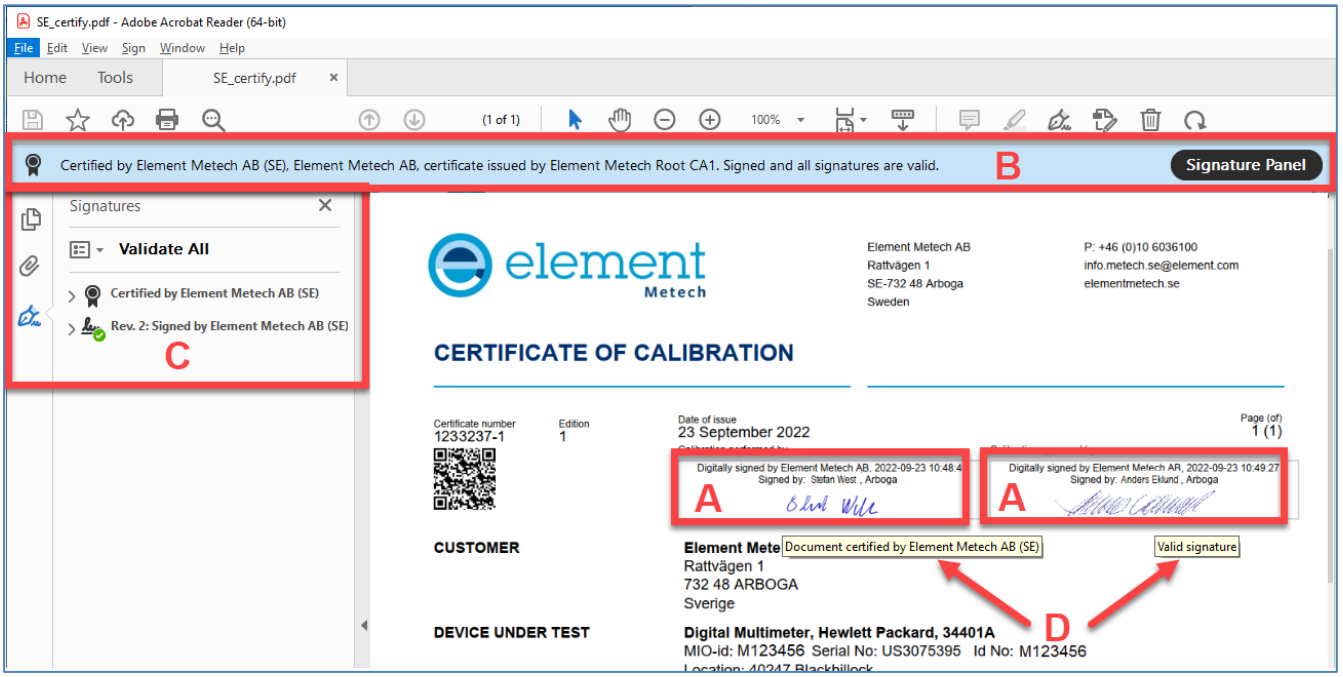
A digital signature can be used to prove that a document was signed by the originator. In addition, a digital signature can also prove that a document has not been modified since it was signed.

A digitally signed document from Element Metech is certified / signed with an Element Metech company certificate, authorized by the signers as performer / approver of the document. The signer is chained to the signature by the Element Metech domain security system. The Element Metech company certificates are chaining up to the Element Metech Root Certificate Authority (CA). The root CA public certificate can then be used, by the recipient, to verify that the signature was performed by an Element Metech company.

When the PDF document is opened in Adobe Acrobat Reader (recommended), the signature(s) is visible in the document (A). If validation is done automatically this will be indicated in the signature ribbon (B). If not, open the signature panel (C) and perform the validation manually or right click a signature field (A) and select "Validate Signature". Validation requires that trust is set for the Element Metech root certificate, see below.

If the mouse pointer is moved over a signature field (A), the tooltip text (D) is visible. The text indicates whether the certification / signature is valid or not.
When two signature fields, the first one is certified by the performer and the second one signed by the approver.

In other PDF readers or versions this may be displayed differently.



How to verify that a document is signed by Element Metech

To verify the signature, you have to download and "Trust" the Element Metech Root CA public certificate. This is done once for each computer or profile, where verification should be possible. For large companies, root certificates can be trusted for the entire network domain. Contact your local IT department.

Download and trust Element Metech digital signatures

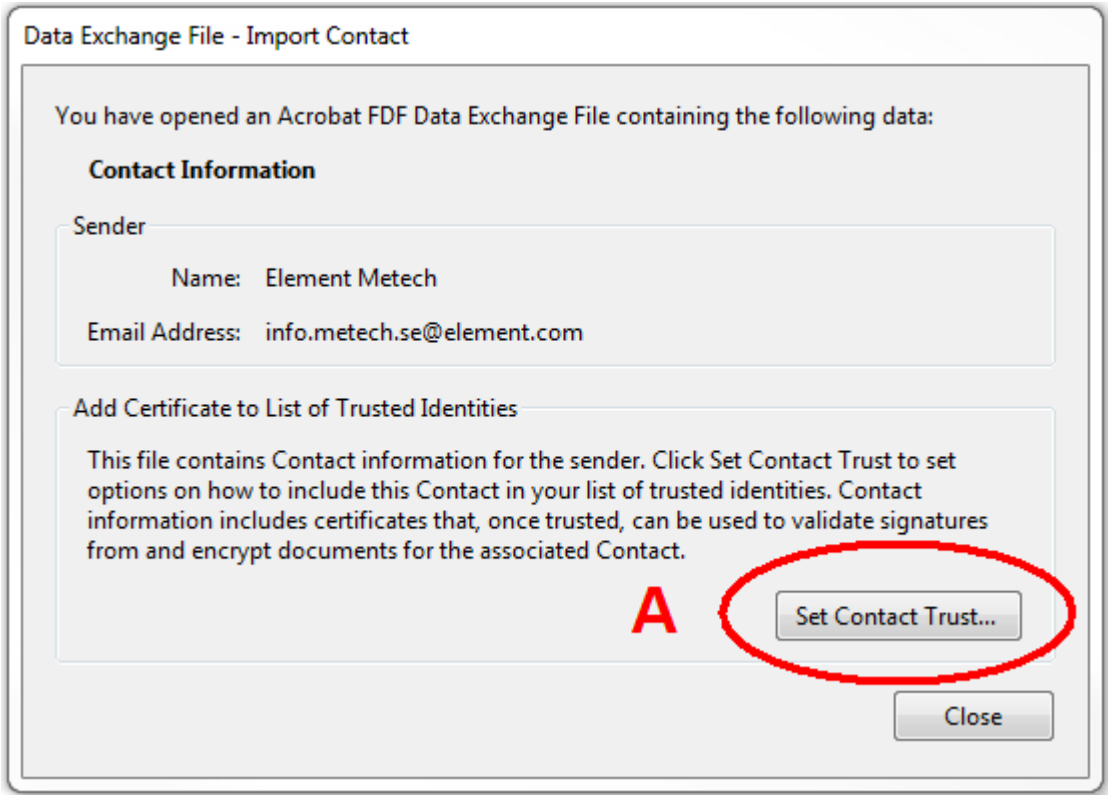
If you are running, the recommended, Adobe Acrobat Reader, download Element Metech Root CA certificate (fdf-file).

For users, not running Adobe Acrobat Reader as PDF reader, download Element Metech Root CA certificate (crt-file) and follow the instructions for your application to trust the certificate.

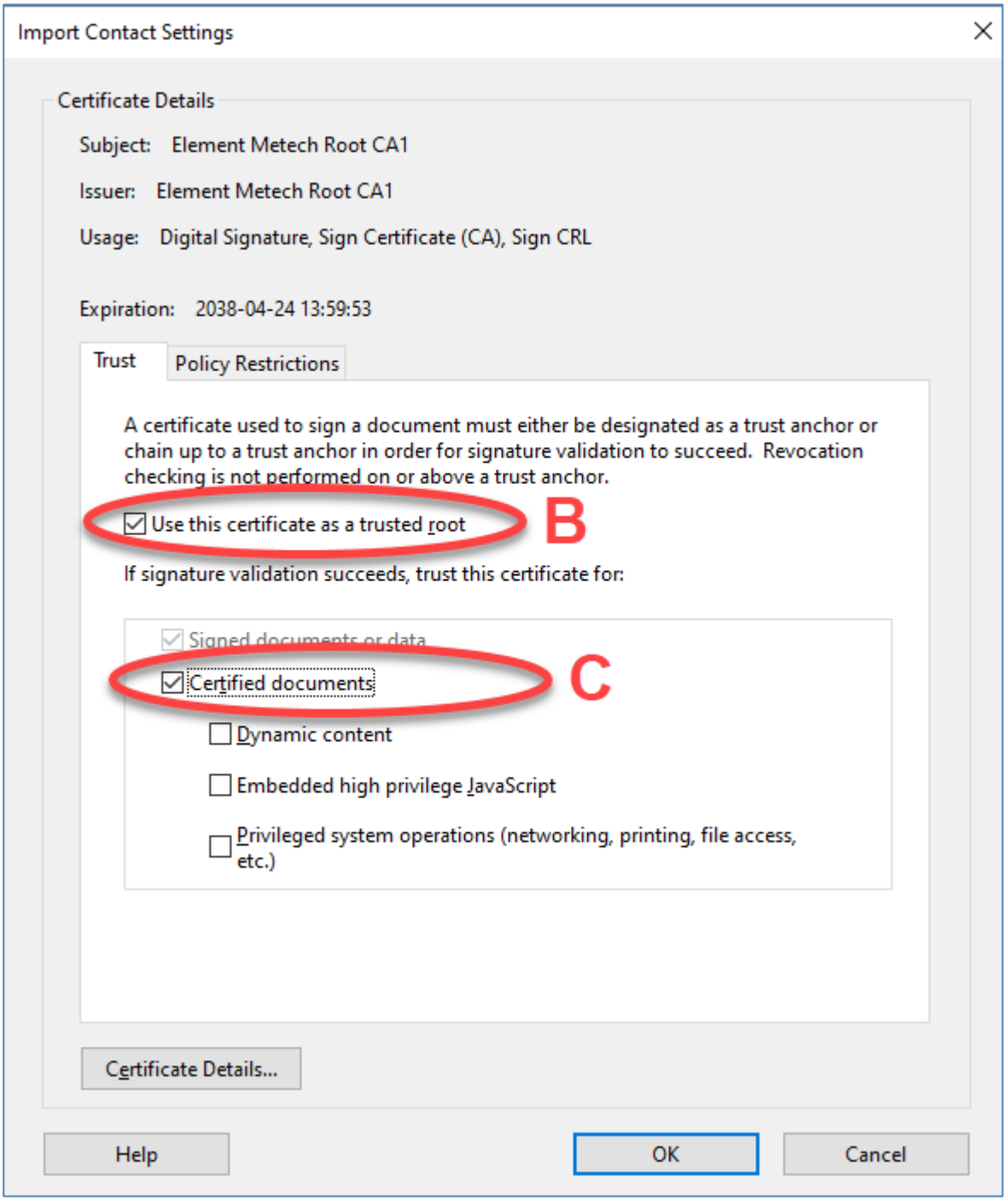
(For certificates signed before 2018-06-25 by Exova Metech, download Exova METECH Root CA certificate (crt-file) or Exova METECH Root CA certificate (fdf-file).)

Use the Adobe Acrobat Reader fdf file to set trust

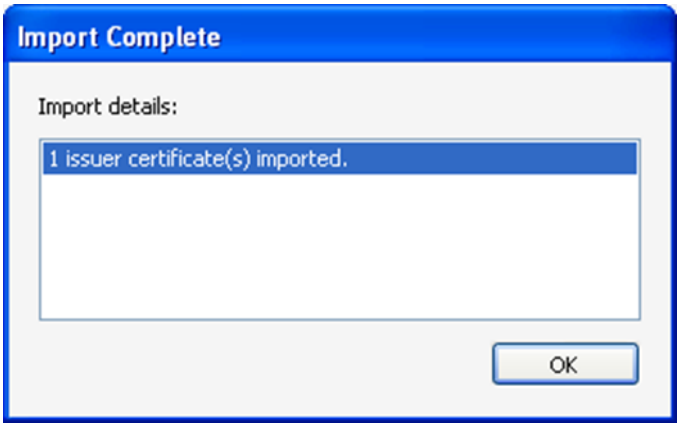
Open the downloaded file, "Element Metech Root CA certificate.fdf", and press **Set Contact Trust** (A).



Tick **Use this certificate as a trusted root** (B)
Tick **Certified documents** (C) and press **OK**



If the import was successful, it should look like the frame below.
Press **OK** to close this frame. Press **Close** to finish the import.
Close the browser window to return to the information site.



The Element Metech Root CA public certificate is now trusted and all Element Metech signed documents, opened on this computer or profile, and validated according to instructions below, should indicate that the signature is valid.

Validate a signature and verify that the document has not been modified

To validate the signature, right click in the signature field, and select "Validate Signature". The Signature Validation Status should then indicate that the signature is VALID and that the document has not been modified. More information can be found by selecting "Show Signature Properties".

Note: Element Metech does not provide Certificate Revocation Lists (CRL) to check for revoked certificates since it is a small number of certificates, and they are only used in a secure server environment.

How does it work technically?

The signer uses a pair of cryptographic keys, a private key and a public key. These keys are contained in certificate files, together with information about the signer. The private key is kept secret by the signer and the public key is published to anyone who needs it.

The signer calculates a "checksum" (hash) for the document to sign. The hash is then encrypted by using the private key. This is the digital signature and is included in the document file. The public key is also included in the document.

The recipient uses the public key to decrypt the hash. If this worked, it proves that the document was signed by the signer's private key. The recipient then calculates the hash for the document and compares it to the decrypted hash, if it is the same, it proves that the document has not been modified.

Element Metech uses a two-tier hierarchy for the certificates (key pairs). The highest level is the root Certificate Authority (CA). The CA uses a self-signed certificate to sign the issued certificates that are actually used to sign documents with. The CA public key can then be used to verify any signature, performed by any of the issued certificates.

To verify that the signature is performed by Element Metech, you must receive the Element Metech Root CA public key. If you are sure that the public key comes from Element Metech, you can import the public key (certificate file) as a trusted root. All certificates signed by Element Metech will then be validated in the PDF reader.