Press release

Natural gas industry accepts CAcert

CAcert is now officially accepted by the Edig@s work group as a trusted Certificate Authority (CA) for Electronic Data Interchange (EDI). This acceptance provides the basis to exchange messages securely between companies utilizing CAcert issued certificates.

Edig@s is the official standard for the grid gas business that covers more than 99% of all western European gas deliveries. It validates the authenticity and the binding character of the contract.

The open CA CAcert offers free advanced electronic signatures for corporate and private use. This makes the usage of CAcert certificates interesting also for small businesses.

94 word 534 characters

1 Press release material

1.1 CAcert

The aim of CAcert is to offer free digital certificates that meet the X.509 standard. These digital certificates can be used to sign and encrypt documents as well as to establish secure data communication links.
The CAcert project has 250,000 registered users. CAcert Inc. is an incorporated non-profit association with approx. 100 members and is registered with New South Wales (NSW), Australia. - It was incorporated by 24 July 2003, with the full association name CAcert Incorporated under the Incorporation No INC9880170. We have a DUNS number 75-605-6102. [2]
CAcert is financed by donations.

[1] https://www.cacert.org/stats.php
[2] https://wiki.cacert.org/CAcertInc

More information:
https://en.wikipedia.org/wiki/CAcert

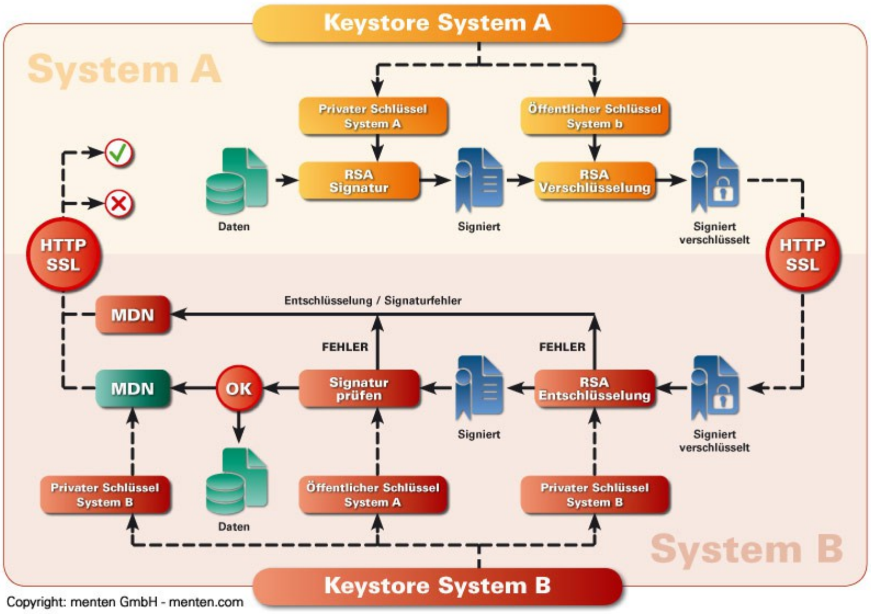
1.2 EDIG@S

Edig@s is an Electronic Data Interchange (EDI) standard for the buying, selling, transporting and storage of gas. It is derived from the UN EDIFACT standard, of which it is an official subset. Edig@s is used almost exclusively in Europe, particularly France, Germany, The Netherlands, Belgium and Scandinavia. Edig@s nominations are either optional or the prime method of nomination to the majority of gas networks in western Europe. Edig@s member networks include, amongst others, Fluxys, GTS, GRTGaz, Gassco and TIGF. In addition several shippers use Edig@s to handle nominations internally. The majority of gas shippers in those markets use "ENOM", a commercially available Edig@s messaging system developed by Gas Management Services Ltd.
https://en.wikipedia.org/wiki/Edig@s

1.3 AS2

AS2 (Applicability Statement 2) is a specification about how to transport data securely and reliably over the Internet. Security is achieved by using digital certificates and encryption.

The AS2 protocol is based on HTTP and S/MIME. It was the second AS protocol developed and uses the same signing, encryption and MDN (as defined by RFC3798) conventions used in the original AS1 protocol introduced in the late 90s by IETF [1]. In other words: Files are encoded as "attachments" in a standardized S/MIME message (an AS2 message).
AS2 messages are always sent using the HTTP or HTTPS protocol (Secure Sockets Layer — also known as SSL — is implied by HTTPS) and usually use the "POST" method (use of "GET" is rare).
Messages can be signed, but do not have to be.
Messages can be encrypted, but do not have to be.
Messages may request a Message Disposition Notification [MDN] back if all went well, but do not have to request such a message.



AS2 diagram http://commons.wikimedia.org/wiki/File:As2_ablauf_zoom.jpg

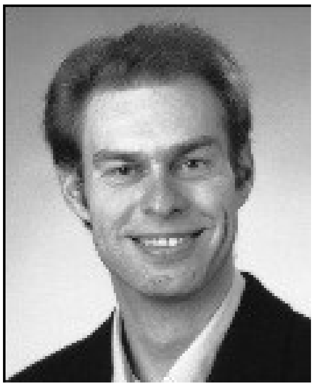
If the original AS2 message requested an MDN: Upon the receipt of the message and its successful decryption or signature validation (as necessary) a "success" MDN will be sent back to the original sender. This MDN is typically signed but never encrypted (unless temporarily encrypted in transit via HTTPS). Upon the receipt and successful verification of the signature on the MDN, the original sender will "know" that the recipient got their message (this provides the "Non-repudiation" element of AS2)

If there are any problems receiving or interpreting the original AS2 message, a "failed" MDN may be sent back. However, part of the AS2 protocol states that the client must treat a lack of an MDN as a failure as well, so some AS2 receivers will simply not return an MDN in this case.

Like any other AS file transfer, AS2 file transfers typically require both sides of the exchange to trade SSL certificates and specific "trading partner" names before any transfers can take place. AS2 trading partner names can usually be any valid phrase.

https://en.wikipedia.org/wiki/AS2

2 Contact CAcert



Alexander Bahlo, Officer for Public Relations
pr@cacert.org