Welcome to IGT and the world of gas regulators. As we care for your security in using our products, we also care about our it-security. A lot actually. So much in fact that we don't take shortcuts and risk our own and our clients data.

Therefore we use CloudPros www.cloudpros.dk . A local Danish no-compromise approach to IT delivery and security.

At Cloudpros they evaluate the incoming email based on SPF, DKIM and DMARC result of an incoming email in order to determine if the From Address can be verified as a trusted sender. If DMARC does not pass, the From Address cannot be used to verify the trusted sender status, and the full spam weight of the email will be applied.

What is SPF?

Sender Policy Framework (SPF) is used to authenticate the sender of an email. With an SPF record in place, Internet Service Providers can verify that a mail server is authorized to send email for a specific domain. An SPF record is a DNS TXT record containing a list of the IP addresses that are allowed to send email on behalf of your domain.

SPF has become exceedingly vital to help verify which sending infrastructure can relay email on behalf of your domain. Implementing SPF for email provides major benefits.

What is DKIM?

DKIM, or DomainKeys Identified Mail, is an email authentication method that uses a digital signature to let the receiver of an email know that the message was sent and authorized by the owner of a domain. Once the receiver determines that an email is signed with a valid DKIM signature it can be confirmed that the email's content has not been modified. In mist cases, DKIM signatures are not visible to end-users, the validation is done on a server level. If DKIM is used together with DMARC, or SPF you can protect your domain against malicious emails sent from domains impersonating your brand.

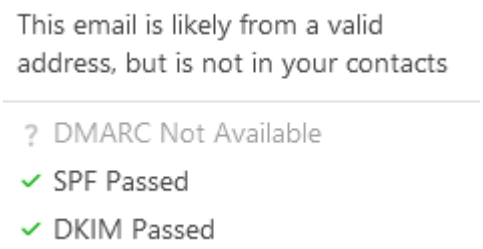
What is DMARC?

DMARC, which stands for "Domain-based Message Authentication, Reporting & Conformance", is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email.<

DMARC is a key component of a brand's email security and deliverability strategy as it enables: Visibility - Monitor emails sent using our domain to ensure they are properly authenticated using SPF and/or DKIM.

IGT Brand Protection - Block spoofed messages that might damage our brand's reputation with customers.

This was made because DMARC is the only check available that can confirm that the From Address listed in the email is associated to the SPF record available. This check ensures that the From Address cannot be spoofed, then automatically trusted just because the From Address is listed as a trusted sender.



In the example we provided, this email had the full spam weight applied because there is no DMARC record available. To correct this issue with the email not being verified as a trusted sender, DMARC must be added by the sender.

Otherwise you can end up in the spamfolder or get the email deleted altogether.

When you get an error when trying to email us at Integrated Gas Technology and it fails, to investigate we need the contents of the error email sent to us via our homepage www.igt-lpg.com where we will provide a contact formular for you to use for the error email.

Sometimes your SMTP server may return a particular error message. The problem is that it will generally be very cryptic, like “550 Requested action not taken: mailbox unavailable” or “421 Try again later”.

What does these numbers mean?

First of all: not any reply code is an error. Sometimes it’s just a response containing a detail about the server or an answer to a command. Secondly: any code consist of three digits, and each conveys a particular information. The first one defines whether the server has accepted the command, fulfilled an action, run into a temporary issue, encountered an error etc; the second and the third one refine the description further, stating if there’s been a syntactic problem, or a connection trouble etc.

Unfortunately, different servers sometimes use these codes in a different way, making the whole thing even more complicated… Anyhow, the most critical series of error messages is the 5xx one, and especially the ones from 550 to 559. In particular, you will probably get a lot of 550 SMTP error codes – that is, a problem that concerns the recipient’s email address.

Finally, remember that it’s much easier to deal with these error codes if you choose to rely on a professional SMTP server that will help you solve any issue. www.cloudpros.dk for instance, comes with a 24/7 customer support: you can use them and forget these issues once and for all.

Look below for the complete list.

And here's a list of the main SMTP error or reply messages, with an explanation and a tip about what to do.

CODE	MEANING	HOW TO SOLVE IT / WHAT TO DO
101	The server is unable to connect.	Try to change the server's name (maybe it was spelt incorrectly) or the connection port.
111	Connection refused or inability to open an SMTP stream.	This error normally refers to a connection issue with the remote SMTP server, depending on firewalls or misspelled domains. Double-check all the configurations and in case ask your provider.
211	System status message or help reply.	It comes with more information about the server.
214	A response to the HELP command.	It contains information about your particular server, normally pointing to a FAQ page.
220	The server is ready.	It's just a welcome message. Just read it and be happy that everything is working (so far)!
221	The server is closing its transmission channel. It can come with side messages like "Goodbye" or "Closing connection".	The mailing session is going to end, which simply means that all messages have been processed.
250	Its typical side message is "Requested mail action okay completed": meaning that the server has transmitted a message.	The oppsite of an error: everything has worked and your email has been delivered.
251	"User not local will forward": the recipient's account is not on the present server, so it will be relayed to another.	It's a normal transfer action.
252	The server cannot verify the user, but it will try to deliver the message anyway.	The recipient's email account is valid, but not verifiable. Normally the server relays the message to another one that will be able to check it.
354	The side message can be very cryptic ("Start mail input end <CRLF>.<CRLF>"). It's the typical response to the DATA command.	The server has received the "From" and "To" details of the email, and is ready to get the body message.
420	"Timeout connection problem": there have been issues during the message transfer.	This error message is produced only by GroupWise servers. Either your email has been blocked by the recipient's firewall, or there's a hardware problem. Check with your provider.

421	The service is unavailable due to a connection problem: it may refer to an exceeded limit of simultaneous connections, or a more general temporary problem.	The server (yours or the recipient's) is not available at the moment, so the dispatch will be tried again later.
422	The recipient's mailbox has exceeded its storage limit.	Best is to contact contact the user via another channel to alert him and ask to create some free room in his mailbox.
431	Not enough space on the disk, or an "out of memory" condition due to a file overload.	This error may depend on too many messages sent to a particular domain. You should try again sending smaller sets of emails instead of one big mail-out.
432	Typical side-message: "The recipient's Exchange Server incoming mail queue has been stopped".	It's a Microsoft Exchange Server's SMTP error code. You should contact it to get more information: generally it's due to a connection problem.
441	The recipient's server is not responding.	There's an issue with the user's incoming server: yours will try again to contact it.
442	The connection was dropped during the transmission.	A typical network connection problem, probably due to your router: check it immediately.
446	The maximum hop count was exceeded for the message: an internal loop has occurred.	Ask your SMTP provider to verify what has happened.
447	Your outgoing message timed out because of issues concerning the incoming server.	This happens generally when you exceeded your server's limit of number of recipients for a message. Try to send it again segmenting the list in different parts.
449	A routing error.	Like error 432, it's related only to Microsoft Exchange.
450	"Requested action not taken – The user's mailbox is unavailable". The mailbox has been corrupted or placed on an offline server, or your email hasn't been accepted for IP problems or blacklisting.	The server will retry to mail the message again, after some time. Anyway, verify that is working on a reliable IP address.
451	"Requested action aborted – Local error in processing". Your ISP's server or the server that got a first relay from yours has encountered a connection problem.	It's normally a transient error due to a message overload, but it can refer also to a rejection due to a remote antispam filter. If it keeps repeating, ask your SMTP provider to check the situation. (If you're sending a large bulk email with a free one that can be a common issue).
452	Too many emails sent or too many recipients: more in general, a server storage limit exceeded.	Again, the typical cause is a message overload. Usually the next try will succeed: in case of problems on your

		server it will come with a side-message like “Out of memory”.
471	An error of your mail server, often due to an issue of the local anti-spam filter.	Contact your SMTP service provider to fix the situation.
500	A syntax error: the server couldn’t recognize the command.	It may be caused by a bad interaction of the server with your firewall or antivirus. Read carefully their instructions to solve it.
501	Another syntax error, not in the command but in its parameters or arguments.	In the majority of the times it’s due to an invalid email address, but it can also be associated with connection problems (and again, an issue concerning your antivirus settings).
502	The command is not implemented.	The command has not been activated yet on your own server. Contact your provider to know more about it.
503	The server has encountered a bad sequence of commands, or it requires an authentication.	In case of “bad sequence”, the server has pulled off its commands in a wrong order, usually because of a broken connection. If an authentication is needed, you should enter your username and password.
504	A command parameter is not implemented.	Like error 501, is a syntax problem; you should ask your provider.
510/511	Bad email address.	One of the addresses in your TO, CC or BBC line doesn’t exist. Check again your recipients’ accounts and correct any possible misspelling.
512	A DNS error: the host server for the recipient’s domain name cannot be found.	Check again all your recipients’ addresses: there will likely be an error in a domain name (like mail@domain.coom instead of mail@domain.com).
513	“Address type is incorrect”: another problem concerning address misspelling. In few cases, however, it’s related to an authentication issue.	Doublecheck your recipients’ addresses and correct any mistake. If everything’s ok and the error persists, then it’s caused by a configuration issue (simply, the server needs an authentication).
523	The total size of your mailing exceeds the recipient server’s limits.	Re-send your message splitting the list in smaller subsets.
530	Normally, an authentication problem. But sometimes it’s about the recipient’s server blacklisting yours, or an invalid email address.	Configure your settings providing a username+password authentication. If the error persists, check all your recipients’ addresses and if you’ve been blacklisted.
541	The recipient address rejected your message: normally, it’s an error caused by an anti-spam filter.	Your message has been detected and labeled as spam. You must ask the recipient to whitelist you.

550	It usually defines a non-existent email address on the remote side.	Though it can be returned also by the recipient's firewall (or when the incoming server is down), the great majority of errors 550 simply tell that the recipient email address doesn't exist. You should contact the recipient otherwise and get the right address.
551	"User not local or invalid address – Relay denied". Meaning, if both your address and the recipient's are not locally hosted by the server, a relay can be interrupted.	It's a (not very clever) strategy to prevent spamming. You should contact your ISP and ask them to allow you as a certified sender. Of course, with a professional SMTP provider like www.cloudpros.dk you won't ever deal with this issue.
552	"Requested mail actions aborted – Exceeded storage allocation": simply put, the recipient's mailbox has exceeded its limits.	Try to send a lighter message: that usually happens when you dispatch emails with big attachments, so check them first.
553	"Requested action not taken – Mailbox name invalid". That is, there's an incorrect email address into the recipients line.	Check all the addresses in the TO, CC and BCC field. There should be an error or a misspelling somewhere.
554	This means that the transaction has failed. It's a permanent error and the server will not try to send the message again.	The incoming server thinks that your email is spam, or your IP has been blacklisted. Check carefully if you ended up in some spam lists.
554.5.3.4	Message to big for system.	You need to contact your vendor to make sure they can send or accept the size of the attachments. Consider that email is not designed for exchange of large files and they should be deleted from the inbox after the receipt.
556	Domain does not accept email.	Server is closed or down for maintenance.

Email Status codes.

This is the codes that give more detail to the overall codes exchanged between mailservers.

For example, if you specify the recipient of the email with the RCPT TO command, the SMTP server may respond with 250 2.1.5 Recipient OK. This code means that not only is your command successful, but the address of the recipient at the server has also been accepted.

SMTP response codes deciphered

SMTP plays a critical role in the email infrastructure of the Internet. It's easy to implement it in your technology stack, but when things go wrong it's hard to decipher what those SMTP codes mean.

The SMTP specification defined basic status codes that were published in 1982. Because the codes were originally designed to report on the outcome of an SMTP command, their lack of detail made them unsuitable for delivery reports.

To make things more complicated, some servers would assign the same error code to different delivery failures. Others would assign a code that only explained its meaning in the text description. Inconsistent application of the codes meant it was difficult to resolve mail sending issues!

Enter the enhanced status codes. They extend the basic status codes by providing more detail about the cause of the email delivery failure. Similarly, they also consist of 3-digit numbers separated by decimals. Let's take a look at how to read them next.

Basic status codes

The first digit of a basic status code tells the sending server whether the response is good, bad or incomplete:

Code	Description	Meaning
2	Positive Completion Reply	The requested action has been successfully completed.
3	Positive Intermediate Reply	The command is accepted but more information is needed before proceeding.
4	Transient Negative Completion Reply	The command was not accepted and no action was taken. This error is seen as temporary (soft bounce) and the sender can try again later.
5	Permanent Negative Completion Reply	The command was not accepted and no action was taken. This is a permanent error (hard bounce) and the sender should not repeat the command.

The second digit puts the SMTP response into a specific category:

0	Syntax	Responses about commands or parameters.
1	Information	Responses to requests for more information.

2	Connections	Responses about the transmission channel.
5	Mail system	Responses about the status of the receiving mail server.

Enhanced status codes

Like the basic status codes, the first digit defines the class to which the code belongs.

2	Success	The requested mail action is okay and completed.
4	Persistent Transient Failure	Temporary conditions will cause the message to be delayed or abandoned.
5	Permanent Failure	The message in its current form cannot be delivered.

The second digit identifies the subject of the SMTP reply code:

0	Other or Undefined Status
1	Addressing Status
2	Mailbox Status
3	Mail System Status
4	Network and Routing Status
5	Mail Delivery Protocol Status
6	Message Content or Media Status
7	Security or Policy Status

This was a little technical walkthrough of the “other” side of email exchange and when everything is configured correctly, we don’t see any issues at all.

As stated before, there are 3 very important things to make sure are working correctly.

SPF (Sender Policy Framework), DKIM signature and DMARC.

When all of these are in place, you don’t end up getting deleted or in a spam folder.

End.