Identity Confirmation

Challenge / Response anti-spam filtering with a twist

❒ Abstract

It is not a matter of novelty to any efficiency-oriented business professional that in nowadays email communication environment, the security issue is not one to ignore. Particularly when talking about the fast-adapting spamming methods which, at the spam-receiving end, can easily be translated as detrimental to the general productivity (therefore wasted) time.

On the other hand, anti-spam measures are constantly implemented, and filters consistently improving. However, the ongoing spam problem has been gaining a lot of ground lately as spammers keep changing tactics frequently enough to make even the best, most adaptive filtering systems unable to cope. The spam-increasing situation has been heavily tackled with for several years now, and strong voices emerged, stating that the best anti-spam approach might not be filtering at all, but a Challenge / Response (C/R) system.

❒ Getting acquainted to C/R anti-spam filtering

For whoever is not very familiar with the term, this approach is based on the simple truth that spam comes from spammers (including mailing robots, spam bots or any automatic mass mailing tool), whereas good mail comes from senders you know (friends, family, business partners, co-workers, the publisher of an email newsletter you have subscribed to). Therefore, it is safe to assume that all “unknown mail” is spam. This is the main idea behind Challenge / Response spam filtering.

Instead of trying to filter out the spam, C/R filters look for mail from trusted senders (those on your so-called "White List") and let it through. Everything else is thought to be spam and “quarantined”. This makes for a fantastic spam detection rate. Moreover, a Challenge / Response system automatically sends a reply with a challenge to the (alleged) sender of every “quarantined” email. In this reply, the sender is asked to perform some action to assure delivery of the original message, which would otherwise not be delivered.

This happens without any effort from the mailbox owner’s part, and, once the address in question is verified, the message is delivered appropriately, as are all subsequent messages from that sender.

Two characteristics that differ between legitimate senders and spammers are exploited in order to ensure the system’s efficiency in protecting from spam. The principle behind the C/R anti-spam method resides in the fact that, while a Challenge / Response request can be easily fulfilled by a real person, it can hardly be performed by a spammer, on the following grounds:

- On the one hand, **legitimate senders have a valid return address** while spammers usually forge a return address. This means that most spammers won't get the challenge, which results in them automatically failing any required action.
- On the other hand, **spammers send email in large quantities** and would have to perform Challenge / Response actions in large numbers, while legitimate senders would only have to perform them once for every new email contact, at the most.

Not only does this sound simple enough and sufficiently elegant, it actually works very well and succeeds in spam-proofing the Inbox efficiently.

❒ Challenge / Response spam filters: what’s out there?

As software developers have been knocking themselves out trying to come up with the killer app that will stop spam forever, and the battle against spam was still spiraling out of control, there were those who realized that the Challenge / Response process is simple, but incredibly efficient, and could represent the simplest solution to the vast majority of spam. So they came up with stand-alone tools, doing expressly, and only, that: Challenge / Response spam filtering, to buy separately and use in addition to an email provider of choice.

We find several such email verification services on the market, some working better than others, but basically doing the same thing, and the similarity is striking. In fact, I came across a single case in which the Challenge / Response anti-spam method is available differently, and in this case it comes as an add-on to a specific messaging solution, and is still regarded as a separately-paid-for option.

It was about time that someone came up with a different approach, one that stands out: an integrated Challenge / Response-based anti-spam system, secure by design, requiring no set up and no effort to use.

❒ Challenge / Response technology. But slightly different.

Axigen Identity Confirmation© is an implementation of a Challenge / Response-based anti-spam method, already embedded in the messaging solution. Starting with version 7.3.0, Axigen Mail Server contains this feature incorporated alongside an existing well-above-average arsenal of anti-spam tools, meeting in full the requirements of the most demanding security-focused professionals, although they’re not the only ones who can easily appreciate this kind of integration at just value.

AXIGEN IDENTITY CONFIRMATION
Challenge / Response AntiSpam filtering at your disposal.
Play Video
Learn how it works

This approach brings Challenge / Response anti-spam filtering at the user’s disposal at only one ‘”enable”-away. Providing the user with his/her own integrated C/R filter certainly seems to set the bar a little bit higher for all mail server software out there that do not offer this kind of upper-level anti-spam protection. Until now, anyone who wanted to benefit from a C/R-based anti-spam filter had to look for a different provider and buy the service separately.

❒ What really makes the difference

There are some elements that distinguish the Axigen Identity Confirmation © from other implementations of Challenge / Response processes, such as:

- The **"Unconfirmed Messages"** folder – where all the received, yet unconfirmed, messages are permanently stored. The unconfirmed emails are available for inspection at anytime, with easy access, without them crowding the Inbox.
- The **"Collected Addresses"** contact folder (part of the Address Book) – where all the confirmed senders are automatically added.
- **Configurable validation code** – at the user's disposal to change whenever they want to.
- The number of days to be skipped **when sending the confirmation request** to a sender – **easy configuration** according to the user's preference.

Moreover, as a Challenge / Response spam-blocking system embodied by a messaging solution, Axigen Identity Confirmation © brings other major upsides to the table:

- It implies **Address Book correlation**, which means no effort put into importing or exporting contacts, and also that any change or update performed Safe Senders list-wise automatically synchronizes with the C/R filter in place.
- Being conceived as **complementary to other anti-spam technology** brings the efficiency of a perfectly coherent extra-layer of security, to result in one of the most extensive security mixes on the market.

So, what really makes Identity Confirmation different in comparison to all other Challenge / Response systems available is the fact that it is already embedded within the messaging solution, with all of the advantages that this incorporation brings, making up a **coherent, hassle-free and comprehensive security package**.

❒ Final thoughts

With this built-in Challenge / Response system, every email received by an Axigen user (who has enabled their Identity Confirmation filter), from anyone who isn't on their Safe Senders list, gets a very easy to fulfill authenticity confirmation request. Messages that pass this challenge, namely those originating with real senders, are delivered to their Inbox. Those that don't, including nearly all spam, aren't. This makes for a very efficient anti-spam method.

And here's the twist: taking into consideration all the advantages brought by such a C/R filter already embedded in the email solution (from the hassle-free Address Book correlation, to its complementary integration with an extensive range of other anti-spam tools), the fact is that Identity Confirmation is, quite simply put, one of the best implementations of Challenge / Response anti-spam filtering out there today.

When adding this to the fact that Axigen Mail Server is the only messaging solution that has augmented their security arsenal to make a Challenge / Response filter effortlessly available, the Identity Confirmation system comes as the perfect extra-layer completing an outstanding security mix, the most extensive currently available.

We invite you to learn more about Identity Confirmation and how it works by simply watching the video. Also, feel free to visit the Security Section on our website, and compare our vision with your security expectations.

AXIGEN cannot be held responsible for any special, collateral or accidental damages, related in any way to the use of this document. AXIGEN does not guarantee either implicitly or explicitly the suitability of this material for your specific needs. This material is provided on an 'as-is' basis.