



COMMUNICATIONS AUTHENTICITY

FOR COMPANIES INTERNAL COMMUNICATIONS OR GENERAL PUBLIC'

COMPANY INTERNAL COMMUNICATION

PROBLEM

- Fake internal email with perfectly spoofed senders asking to urgently wire money.
- Fake email from suppliers communicating “new bank coordinates”.
- Calls for donations that look from your organization, but are not.

If you have not been targeted - yet- probably someone you know has been a victim of these increasing common scams.

SOLUTION - ARMILIS AUTHENTICATOR

SEAMLESS EXPERIENCE

SENDER

Write the email content and attach a document (optional) inside the Authenticator app and hit “Sign”. The content will be passed to your email or instant messaging client of your choice ready to be sent.

RECIPIENT

Along with your email, the recipient will receive a link that displays our on-line tool for instant verification of the sender’s identity and email content.

HOW IT WORKS

SENDER SIDE

The Authenticator app generates a unique pair of Secret and Public keys. The Secret key never leaves your device and the Public key allows others to verify your signature (but not to forge it). When done composing in the email, all its content (text and attachments) are signed using Secret key and a verification link is added to the message body.

BLOCKCHAIN SIDE

When the message is signed, a blockchain record containing the fingerprint of the message and the location of the Public key, pre-shared on your company’s server, is created. The link in the message body points to this unique identifier.



This blockchain record doesn't leak any information about the message itself nor the location of your public key.

VERIFICATION PROCESS

In the page opened by the verification link, the following sender information is shown and verified:

- The identity of the sender, as stated in the Identity Certificate of the company's page holding the verification key.
- The fingerprint of any attachment.
- A textbox where to copy-paste the body of the message. The tool compares this content's fingerprint with the one saved in blockchain, authenticating or rejecting it.

This passage can be custom-implemented by your company since both the blockchain and the signature scheme are public.

COMMUNICATIONS TO THE GENERAL PUBLIC

PROBLEM

- Fake news coming from unverifiable senders.
- Falsified data and media content to create misinformation and bias.

This is specially the case for news coming from other countries or about situations that impact globally (pandemic, wars, elections, ...)

SOLUTION - ARMILIS AUTHENTICATOR

SEAMLESS EXPERIENCE

COMPANY

The message to be released to the public (social media post or document) is signed with the Authenticator and a verification link is attached to it.

THE WORLD

Readers can then verify the content by clicking the link. This will show a short text confirming its authenticity.

HOW IT WORKS

SENDER SIDE

The Authenticator app generates a unique pair of Secret and Public keys. The Secret key never leaves your device and the Public key allows others to verify your signature (but not to forge it). When done composing in the email, all its content (text and attachments) are signed using Secret key and a verification link is added to the message body.

BLOCKCHAIN SIDE

When the message is signed, a blockchain record containing the fingerprint of the message and the location of the Public key, pre-shared on your company’s server, is created. The link in the message body points to this unique identifier.



This blockchain record doesn't leak any information about the message itself nor the location of your public key.

VERIFICATION PROCESS

In the page opened by the verification link, the following sender information is shown and verified:

- The identity of the sender, as stated in the Identity Certificate of the company's page holding the verification key.
- The fingerprint of any attachment.
- A textbox where to copy-paste the body of the message. The tool compares this content's fingerprint with the one saved in blockchain, authenticating or rejecting it.

This passage can be custom-implemented by your company since both the blockchain and the signature scheme are public.
