

ABSTRACT OF THE DISCLOSURE

METHODS AND SYSTEMS FOR PKI-BASED AUTHENTICATION

Methods, systems, and devices are provided for authenticating API messages using PKI-based authentication techniques. A client system can generate a private/public key pair associated with the client system and sign an API message using the private key of the private/public key pair and a PKI-based cryptographic algorithm, before sending the signed API message to a server system. The server system (e.g., operated by a service provider) can authenticate the incoming signed API message using a proxy authenticator located in less trusted zone (e.g., a perimeter network) of the server system. In particular, the proxy authenticator can be configured to verify the signature of the signed API message using the public key corresponding to the private key and the same cryptographic algorithm. The authenticated API message can then be forwarded to a more trusted zone (e.g., an internal network) of the server system for further processing.

FIG. 1