

Preliminary

Secure Anonymous Authentication using a Monero Wallet

02 May 2018

Introduction

This paper documents our new protocol for securely authenticating to a digital resource using a Monero wallet. The object for authentication is a Monero address. A Monero address is the identifier presented to a system for authentication.

First, an entity makes an authentication request and is presented with a *challenge phrase* by the system. The system managing the authentication process, expects the entity requesting authentication, to digitally sign the challenge phrase with a specific Monero address. After presenting the challenge phrase to the requester, the system waits to receive:

- challenge phrase
- Monero address
- Signature

from the requester. Once the above information is provided to the system, the system verifies the digital signature. If the signature is valid, authentication is successful. If the signature does not validate, the authentication request is denied.

A valid signature proves to the system that the requester holds the private key for the provided Monero address.

The protocol consists of two events and the passing of two messages in the authentication methodology:

The first event is a request for authentication.

Once a request for authentication is received by the system, the system responds with a challenge phrase.

When the entity requesting authentication receives the challenge phrase, the challenge phrase is signed with a Monero wallet.

Once the challenge phrase is signed, the challenge phrase, Monero address, and the signature are passed to the system

The system then validates the signature with a Monero wallet. The result of the validation generates an authorization event. Authorization is a pass (true) or fail (false) event.

When we say anonymous authentication, it is in reference to the identity of the entity that holds the private key for the Monero address that is the object of authentication.

The *identity* for the entity requesting authentication is always a unique Monero address and in order to pass authentication, the entity requesting authentication must possess the private key of the Monero address in order to generate a valid signature for the challenge phrase.

