February 04, 2019

VERIFIABLY SECURE SESSION INITIATION PROTOCOL REQUESTS

Mark Barrasso

VERIFIABLY SECURE SESSION INITIATION PROTOCOL REQUESTS

AUTHORS:
Mark Barrasso

ABSTRACT

Techniques are described for reducing the amount of spam and congestion on Session Initiation Protocol (SIP) devices and endpoints to significantly improve customer User Experience (UX). This may be packaged as a web Application Programming Interface (API) that provides an "anti-spam as a service" for other web-based clients.

DETAILED DESCRIPTION

According to a recent Federal Trade Commission (FTC) report, more people are being harassed by call spoofers and spammers than ever before. Anyone is able to download a call spoofing program that enables clients to deliberately falsify the information transmitted to caller Identification (ID) in order to disguise their identity. Many efforts to prevent this problem have so far proven ineffective.

Described herein is an eco-friendly method for User Agent Clients (UACs) to easily obtain a provably trusted certificate before initiating a SIP request.

Clients may follow a series of steps at call setup time. First, the UAC validates their domain by requesting a new certificate. Second, the UAC deposits funds into a root chain contract. This is the smart contract that contains the application's relevant business logic and terms. Third, the operator of the child chain service listens for deposit events that are executed on the root chain, and creates a new block which assigns an amount of SIP tokens to the UAC's address. Fourth, the UAC is now able to perform calls by submitting transactions to the operator which include the following data: the recipient's SIP address, a zero-knowledge proof of the sender's authenticity (e.g., a proof containing the certificate), and a monetary bond to act as collateral (e.g., one SIP token). Fifth, the User Agent Service (UAS) and child chain operator are both able to verify the legitimacy of the UAC by checking the publicly available certificate against the submitted proof of authenticity.

The operator will periodically commit a hash of the state of the child chain to the root chain in order to inherit the security guarantees of the root chain. The UAC is

disincentivized to misbehave since anyone can submit a Merkle proof that shows the invalid state of the child chain. The UACs may be slashed and lose their collateral.

Figure 1 below illustrates an example overview.

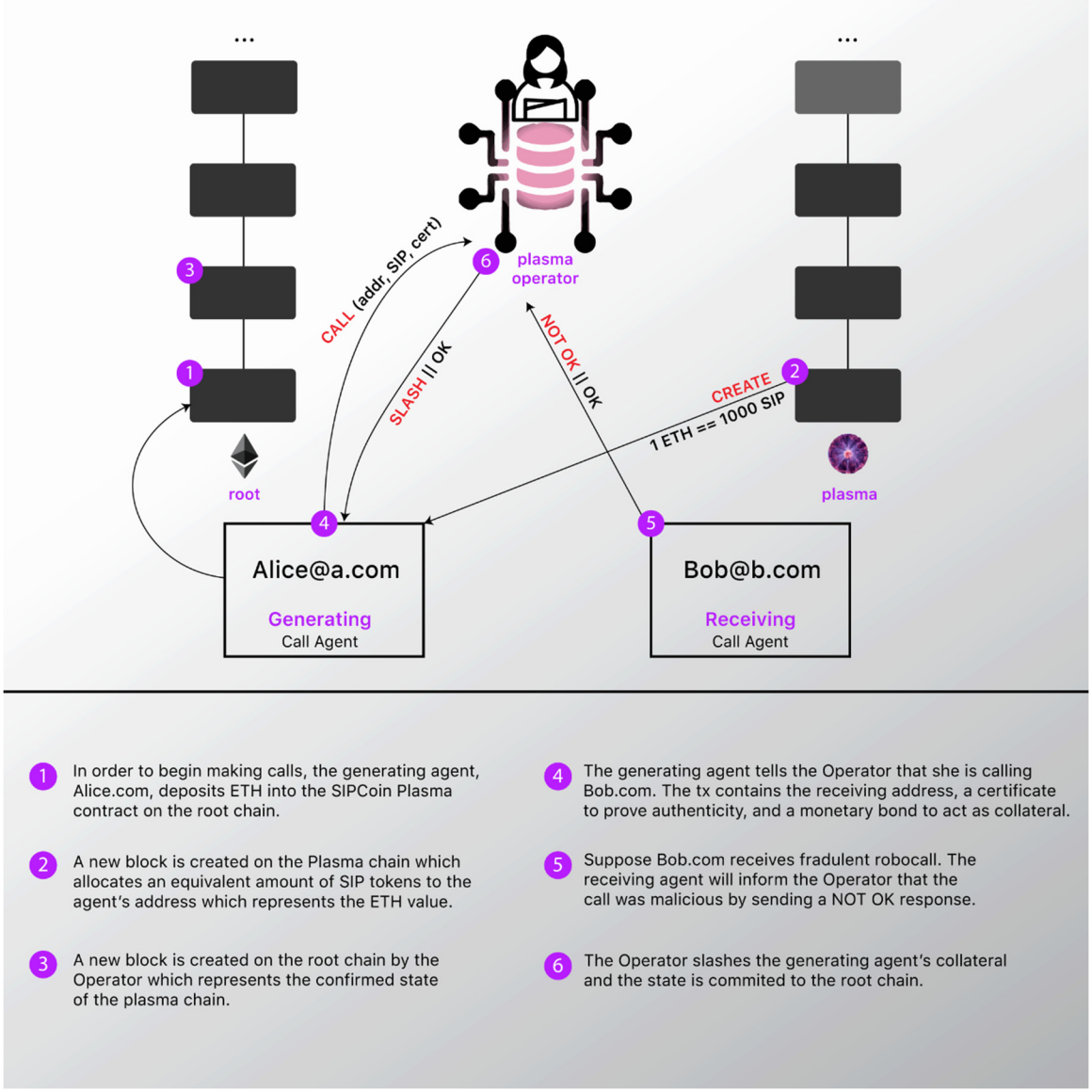

Figure 1

Figure 2 below illustrates an example architecture.

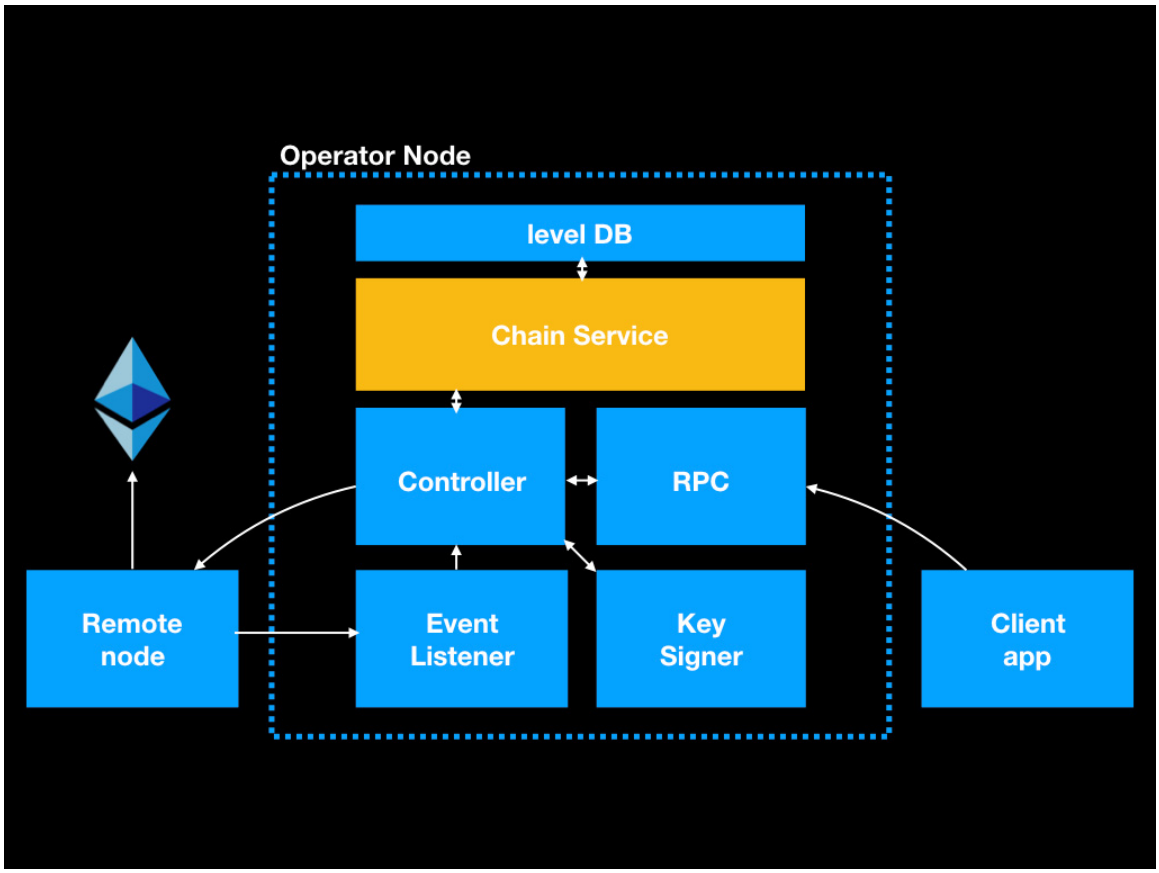

Figure 2

Figure 3 below illustrates an example call intent sequence.

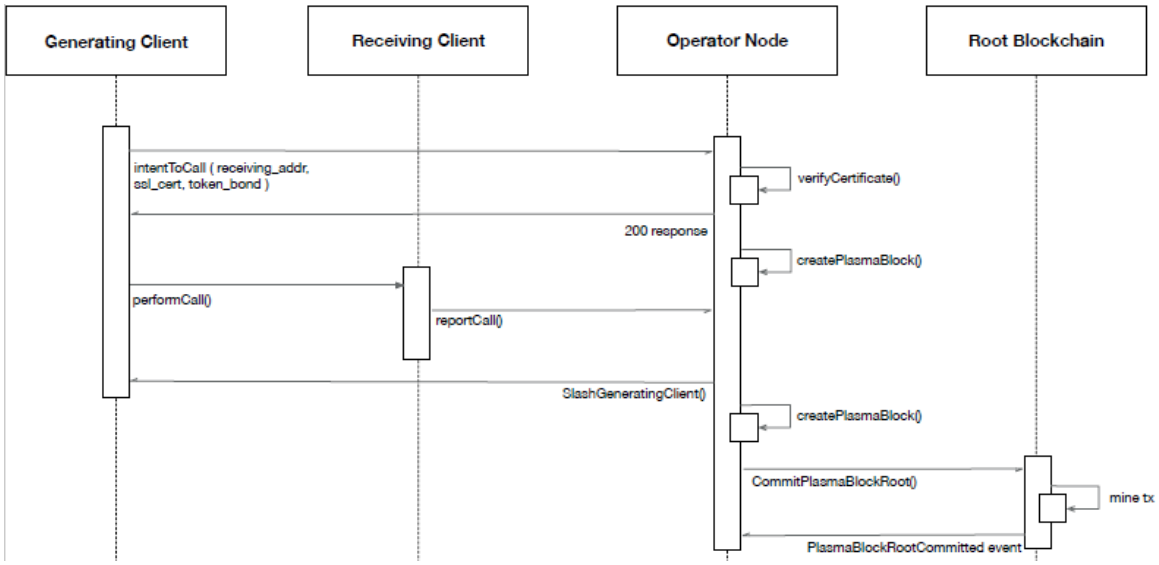

Figure 3

Figure 4 below illustrates an example deposit sequence.

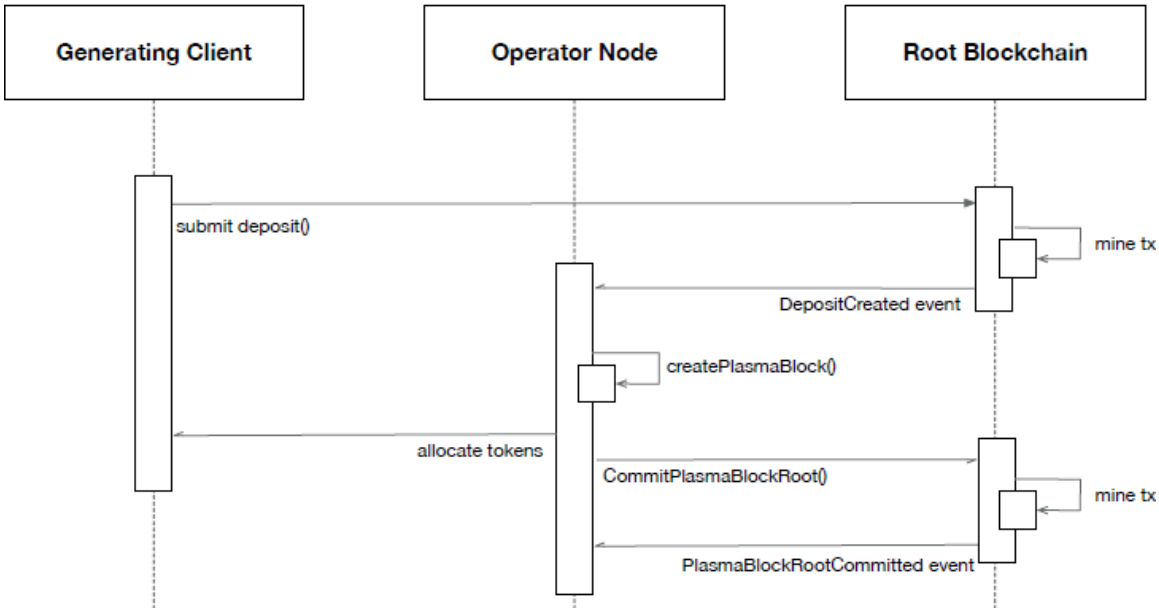

Figure 4

In summary, techniques are described for reducing the amount of spam and congestion on SIP devices and endpoints to significantly improve customer User Experience (UX). This may be packaged as a web Application Programming Interface (API) that provides an "anti-spam as a service" for other web-based clients.