EIP 712: Ethereum typed structured data hashing and signing (DRAFT)

Return to Ethereum ERCs

: **Note**: The following is an excerpt from the official Ethereum site. It is provided here as a connivence and is not authoritative. Refer to the original document as the authoritative reference.

Table 1: Data sheet for Ethereum typed structured data hashing and signing

Title	Ethereum typed structured data hashing and signing
Author	Remco Bloemen, Leonid Logvinov, Jacob Evans
Status	Draft
Created	2017-09-12
Description	http://eips.ethereum.org/EIPS/eip-712
Specification	http://eips.ethereum.org/EIPS/eip-712#Specification
Category	Interface
Requires	EIP 155, EIP 191

Simple Summary

Signing data is a solved problem if all we care about are bytestrings. Unfortunately in the real world we care about complex meaningful messages. Hashing structured data is non-trivial and errors result in loss of the security properties of the system.

As such, the adage “don’t roll your own crypto” applies. Instead, a peer-reviewed well-tested standard method needs to be used. This EIP aims to be that standard.

Abstract

This is a standard for hashing and signing of typed structured data as opposed to just bytestrings. It includes a

- *theoretical framework for correctness of encoding functions,*
- *specification of structured data similar to and compatible with Solidity structs,*
- *safe hashing algorithm for instances of those structures,*
- *safe inclusion of those instances in the set of signable messages,*
- *an extensible mechanism for domain separation,*
- *new RPC call eth_signTypedData, and*

- *an optimized implementation of the hashing algorithm in EVM.*

  It does not include replay protection.