

verifyZkloginSignature

Verify a zkLogin signature based on the provided transaction or personal message based on current epoch, chain id, and latest JWKs fetched on-chain. If the signature is valid, the function returns a `ZkLoginVerifyResult` with success as true and an empty list of errors. If the signature is invalid, the function returns a `ZkLoginVerifyResult` with success as false with a list of errors.

- `bytes` is either the personal message in raw bytes or transaction data bytes in BCS-encoded and then Base64-encoded.
- `signature` is a serialized zkLogin signature that is Base64-encoded.
- `intentScope` is an enum that specifies the intent scope to be used to parse bytes.
- `author` is the address of the signer of the transaction or personal msg.

```
verifyZkloginSignature(  
  bytes: Base64!  
  signature: Base64!  
  intentScope: ZkLoginIntentScope!  
  author: SuiAddress!  
): ZkLoginVerifyResult!
```

Arguments

`verifyZkloginSignature.bytes` • `Base64!` **non-null** **scalar**

`verifyZkloginSignature.signature` • `Base64!` **non-null**
scalar

`verifyZkloginSignature.intentScope` • `ZkLoginIntentScope!`
non-null **enum**

`verifyZkloginSignature.author` • `SuiAddress!` **non-null**
scalar

Type

`ZkLoginVerifyResult` **object**

The result of the zkLogin signature verification.



© 2025 SUI FOUNDATION | DOCUMENTATION DISTRIBUTED UNDER CC BY 4.0