

signature , , , hashToVerify.

URL-

<https://signer.cipher.kiev.ua/api/v1/ticket/{uuid}/ds/verifier/hash>

POST

uuid	String	
------	--------	--

Content-Type	application/json
--------------	------------------

JSON

hashToVerify	String	, .	Base64 .
signature	String	.	Base64 .

	Content-type		
200	application/json	message verifyResults	{ "message" : " .", "verifyResults" : Array }
503	application/json	message	{ "message" : " ." }
400	application/json	message	{ "message" : " ." }
406	application/json	message verifyResults failureCause	{ "message" : " .", "failureCause" : "", "verifyResults" : Array }

JSON

message	String	
failureCause	String	,
verifyResults	Array	

verifyResults

status	String	"SUCCESS" - "FAILURE" -

failureCause	String	,
signerInfo	Object	
signingDateTime	String	
isValid	Boolean	true - false -
contentTimestamp	Object	() ,
signatureTimestamps	Array	
isUntrustedValid	Boolean	, . true - false -
signatureType	String	. : • DETACHED • ATTACHED • ASIC_S • ASIC_E
signatureFormat	String	. : • CADES_BES • CADES_C • CADES_T • CADES_X_LONG • XADES_B_B • XADES_B_T • XADES_B_LT • XADES_B_LTA

contentTimestamp, signatureTimestamps

isValid	Boolean	true - false -
isFailure	Boolean	true - false -
dateTime	DateTime	ISO 8601,
tsaCertificateSerialNumber	Object*	TSP-

signerInfo

ownerCertificateInfo	Object*	
issuerCertificateInfo	Object*	
publicKeyCertificateInfo	Object*	
certificateSerialNumber	Object*	
notBefore	Object*	
notAfter	Object*	
extensionsCertificateInfo	Object*	

signerInfo.ownerCertificateInfo.value

ownerSurname	Object*	

ownerGivenname	Object*	
ownerFullName	Object*	
ownerCountry	Object*	
ownerRegion	Object*	
ownerCity	Object*	
ownerAddress	Object*	
ownerSerialNumber	Object*	
ownerPosition	Object*	

signerInfo.issuerCertificateInfo.value

issuerOrganization	Object*	
issuerDepartment	Object*	
issuerFullName	Object*	
issuerCountry	Object*	
issuerRegion	Object*	
issuerCity	Object*	
issuerAddress	Object*	
issuerSerialNumber	Object*	

signerInfo.publicKeyCertificateInfo.value

publicKey	Object*	
dsAlgorism	Object*	

signerInfo.extensionsCertificateInfo.value

personalData	Object*	
alternativeOwnerName	Object*	
subjectKeyId	Object*	
issuerKeyId	Object*	
subjectOwnerId	Object*	
certificateProfile	Object*	
keyUsage	Object*	
isTemporary	Object*	
isReinforced	Object*	
isQualified	Object*	
isPrivateKeyOnQSCD	Object*	
qscdTypeName	Object*	
isElectronicStamp	Object*	

signerInfo.extensionsCertificateInfo.value.personalData.value

customId	Object*	
passport	Object*	
drfou	Object*	
edrpou	Object*	
eddrun	Object*	

Object*

description	String	,
value	[Object, String, Boolean, Number, Array, null]	

signerInfo

```
{
  "message": " .",
  "verifyResults": [
    {
      "status": "SUCCESS",
      "failureCause": "",
      "isValid": true,
      "signingDateTime": "2020-03-05T13:25:36Z",
      "contentTimestamp": {},
      "signatureTimestamps": [
        {
          "isValid": true,
          "isFailure": false,
          "dateTime": "2020-03-05T13:25:39Z",
          "tsaCertificateSerialNumber": "3DB73E7BF0D575B20200000001000000BB000000"
        }
      ]
    },
    "signerInfo": {
      "ownerCertificateInfo": {
        "description": "",
        "value": {
          "ownerSurname": {
            "description": "",
            "value": ""
          },
          "ownerGivenname": {
            "description": " -",
            "value": " "
          },
          "ownerFullName": {
            "description": " ",
            "value": " "
          },
          "ownerCountry": {
            "description": "",
            "value": "UA"
          },
          "ownerRegion": {
            "description": "",
            "value": null
          },
          "ownerCity": {
            "description": "",
            "value": ""
          },
          "ownerAddress": {
            "description": " ",
            "value": null
          }
        }
      },
    },
  ],
}
```

```

        "ownerSerialNumber": {
            "description": " ",
            "value": "2423814"
        },
        "ownerPosition": {
            "description": "",
            "value": null
        },
        "ownerOrganization": {
            "description": "",
            "value": null
        },
        "ownerOrganizationUnit": {
            "description": " ()",
            "value": null
        }
    },
    "issuerCertificateInfo": {
        "description": "",
        "value": {
            "issuerOrganization": {
                "description": "",
                "value": "- "
            },
            "issuerDepartment": {
                "description": "",
                "value": " () "
            },
            "issuerFullName": {
                "description": " '",
                "value": " "
            },
            "issuerCountry": {
                "description": "",
                "value": "UA"
            },
            "issuerRegion": {
                "description": "",
                "value": null
            },
            "issuerCity": {
                "description": "",
                "value": ""
            },
            "issuerAddress": {
                "description": " ",
                "value": null
            },
            "issuerSerialNumber": {
                "description": " ",
                "value": "UA-39384476-2018"
            }
        }
    },
    "publicKeyCertificateInfo": {
        "description": " ",
        "value": {
            "publicKey": {
                "description": " ",
                "value": "C4 39 B0 5D 95 8A 6D 95 0E 4D F4 71 2A 62 59 6B A1 55 C9 6A 91 99 21 01
8E D3 7B B4 72 11 E6 F9 00"
            },
            "dsAlgorism": {
                "description": " ",
                "value": " 4145-2002, , little-endian"
            }
        }
    },
    "certificateSerialNumber": {
        "description": " ",

```

```
    "value": "20B4E4ED0D30998C0400000006FC24004DAD7500"
  },
  "notBefore": {
    "description": " ",
    "value": "2019-06-10T21:00:00Z"
  },
  "notAfter": {
    "description": " ",
    "value": "2021-06-10T21:00:00Z"
  },
  "extensionsCertificateInfo": {
    "description": "",
    "value": {
      "personalData": {
        "description": " ",
        "value": {
          "customId": {
            "description": " ",
            "value": null
          },
          "passport": {
            "description": " ",
            "value": null
          },
          "drfou": {
            "description": " ",
            "value": "2031914098"
          },
          "edrpou": {
            "description": " ",
            "value": null
          },
          "eddrun": {
            "description": " ",
            "value": null
          }
        }
      },
      "alternativeOwnerName": {
        "description": " ' ",
        "value": null
      },
      "subjectKeyId": {
        "description": " ",
        "value": "9E 03 BA B2 24 4C 3D 02 09 41 08 8E 7E A3 E8 81 CD C6 90 58 B5 9B 38 1F
90 98 DC 5D F3 EF 61 8E"
      },
      "issuerKeyId": {
        "description": " ",
        "value": "20 B4 E4 ED 0D 30 99 8C BE 30 6A 07 7D 69 9A 32 73 23 8A E9 09 08 71 D6
16 37 0E 18 E5 76 D4 7F"
      },
      "subjectOwnerId": {
        "description": " ",
        "value": "00"
      },
      "certificateProfile": {
        "description": " ",
        "value": null
      },
      "keyUsage": {
        "description": " ",
        "value": " , "
      },
      "isTemporary": {
        "description": "",
        "value": "false"
      },
      "isReinforced": {
        "description": "",
        "value": "true"
      }
    }
  }
}
```

```
    },
    "isQualified": {
      "description": "",
      "value": "true"
    },
    "isPrivateKeyOnQSCD": {
      "description": " ",
      "value": "false"
    },
    "qscdTypeName": {
      "description": " ",
      "value": null
    },
    "isElectronicStamp" : {
      "description": " ",
      "value": "false"
    }
  }
}
]
```