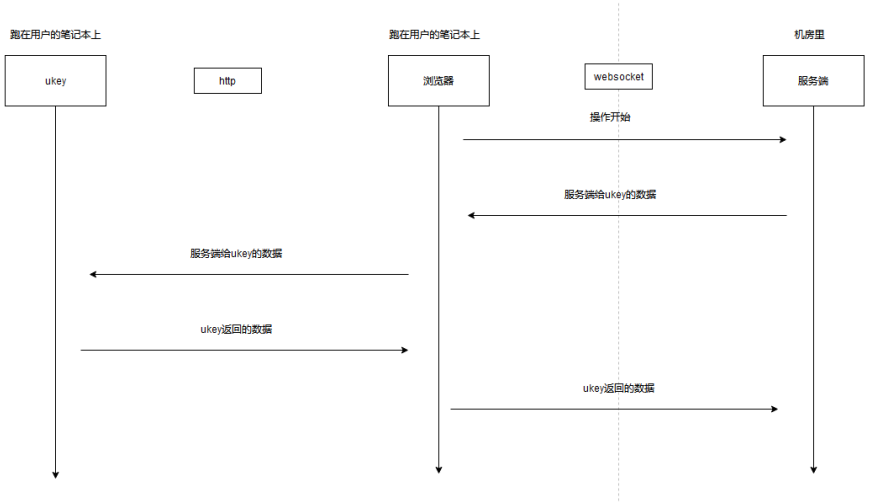
ukey调用流程

ukey & 浏览器 & 中心服务端调用流程



验证 Ukey 流程：

操作开始：浏览器 -> 服务端

```
 {
  "type": "http_request",
  "path": "/ukey/verify",
  "headers": {
    "entity-token": "eyJhbGciOiJIUzUxMiJ9.
eyJpZCI6IjEiLCJ0eXBlIjoid2ViLXVzZXIiLCJleHAiOjE3MjgwMjQ4ODcsInJhbmRvbS1mYWN0b3IiOiIxOThlODg0Yi00NTU3LTQ3MDItODJi
Ni0zNjY4ZjdlOGM5ZmYifQ.Fgk_siI88JDffSMP4ErLTej7i-9ts2MF0jrNz6TZdILgfhup0JcNkEZ2CUR94W929E1fPhauQLKvjtUq9bhqxw"
  }
}
```

服务端给 ukey 的数据：服务端 -> 浏览器

```
 {
  "type": "ukey_request",
  "content": {
    "session": "a6KReNPuRrXFDCnlMT+VCid/AGC6i9liBfoltgM+sAI=",
    "type": "verify" // ukeytype
  }
}
```

浏览器 -> ukey

浏览器将此数据连同 pincode 转交给 ukey

http://ip:host/ukey/api/v1

```
 {
  "type": "verify",
  "pincode": "", //  pincode  mask  pincodemask  ukey
  "session": "" //    session
}
```

ukey 返回的数据：浏览器 -> 服务端

浏览器拿到 ukey 返回的数据过后，将其传递给服务端

以下为 ukey 返回的数据格式：

```
 {
  "uuid": "ukey-1",
  "session": "a6KReNPuRrXFDCnlMT+VCid/AGC6i9liBfoltgM+sAI=",
  "signature": "MEUCIHVig
/94izSLWzhn4dPPaDBZMoZ0MHfhvyw73gGUdHqzAiEArbwo872YVza1j7tkRuj0ZhAFpWtl26R95OSKqH4r3HE="
}
```

以下是浏览器发给服务端的数据的格式：

```
 {
  "type": "ukey_response",
  "content": {
    "uuid": "ukey-1",
    "session": "a6KReNPuRrXFDCnlMT+VCid/AGC6i9liBfoltgM+sAI=",
    "signature": "MEUCIHVig
/94izSLWzhn4dPPaDBZMoZ0MHfhvyw73gGUdHqzAiEArbwo872YVza1j7tkRuj0ZhAFpWtl26R95OSKqH4r3HE="
  }
}
```

操作结果

如果操作结果成功，服务端返回以下数据给浏览器：

```
 {
  "type": "http_response",
  "content": {
    "code": "SUCCESS"
  }
}
```

如果过程中出错，那么服务端将通过 content.code 传递不同的错误码给浏览器，例如：USER_NOT_BOUND_WITH_ANY_UKEY，VERIFY_FAILED 等。

绑定 Ukey 流程：

操作开始：浏览器 -> 服务端

```
 {
  "type": "http_request",
  "task_id": 10000001,
  "path": "/ukey/bind",
  "headers": {
    "entity-token": "eyJhbGciOiJIUzUxMiJ9.
eyJpZCI6IjEiLCJ0eXBlIjoid2ViLXVzZXIiLCJleHAiOjE3Mjc5NjE0MTMsInJhbmRvbS1mYWN0b3IiOiI1M2U2MDk5Mi1hODQ2LTQyN2YtOTcx
Mi0xMDU5N2EwNmNmYmMifQ.PNWAjY8SFT_2RAmkfv0iEiD9zEGosvotEPRQudRGItTxL-nDW8ktfBkZ5pvuZyQ3a6ogRtIb5mZvtSY2MYAB-A"
  },
  "content": {
    "mode": "self" // self/other selfukeyotherukey; api
  }
}
```

服务端给 ukey 的数据：服务端 -> 浏览器

```
 {
  "type": "ukey_request",
  "content": {
    "server_enc_pk":
"MFkwEwYHKoZIzj0CAQYIKoEcz1UBgi0DQgAEUD6tDRXahnqPrKvCVc0sQtGPgzo1GCJZto+M0ckd+gZNjFpeHLdmUNRCcBSxvcZtDKKXLlmW7u9
jvNoQGNVKfQ==",
    "type": "init"
  }
}
```

浏览器 -> ukey

浏览器将此数据连同 pincode 转交给 ukey

http://ip:host/ukey/api/v1

```
 {
  "type": "init",
  "pincode": "", //  pincode  mask  pincodemask  ukey
  "server_enc_pk": "" //    session
}
```

ukey 返回的数据：浏览器 -> 服务端

浏览器拿到 ukey 返回的数据过后，将其传递给服务端

以下为 ukey 返回的数据格式：

```
 {
  "uuid": "ukey-1",
  "sign_pk": "MIHDAiAGtCMMbiaoQrhTBN06EavjZnNJQR86Ff0fL/NMXJvhYgIgPRLvEorfVefx
/Fl4LzqTqitqCD7jgrb0G6EqrNhVGHEEIF1OTIbXCKOpu4aiIpVnrXzV9YUYAvLQK4pb8z6nqJHMBFtwVShc6gBSYKQWa3tEfvilAUeIAqiDBcmu
uIcS9NWobYdIpSIsKnVlSZ2RAhyMXl26DjpoqA3/OjL4RaBUO05Wgn3sCfbIGv1lrc8tLvokybhbx+G0E6dhN/n2",
  "enc_pk": "MIHFAiEA9eQWGD2KcgiFdw3pUU1l1XJRQ2
/2K4CcNsPsrs8Ns0gCIQCk70SQQpD7hqNffzbZsJCw4hF2DZJRmAT5V4nCyAegfQQgfRJt66Wx7mW2LssKeyE8lb7BXpkog5Kk9yzpbUH
/PSQEW5eHqlPDnuklTz9xkMLWE7dkxpLHGC9e0u53
/VCTeCpPnqH1A3yTrkyI8ASpv9X70JldyHJkmJb0BrBiningTZmL0KAXvGLuWsdqvJUOikJW5QvSPI/HlO0vDC4="
}
```

以下是浏览器发给服务端的数据的格式：

```
 {
  "type": "ukey_response",
  "task_id": 1000000,
  "content": {
    "uuid": "ukey-1", // bind this uuid to user
    "sign_pk": "MIHDAiAGtCMMbiaoQrhTBN06EavjZnNJQR86Ff0fL/NMXJvhYgIgPRLvEorfVefx
/Fl4LzqTqitqCD7jgrb0G6EqrNhVGHEEIF1OTIbXCKOpu4aiIpVnrXzV9YUYAvLQK4pb8z6nqJHMBFtwVShc6gBSYKQWa3tEfvilAUeIAqiDBcmu
uIcS9NWobYdIpSIsKnVlSZ2RAhyMXl26DjpoqA3/OjL4RaBUO05Wgn3sCfbIGv1lrc8tLvokybhbx+G0E6dhN/n2",
    "enc_pk": "MIHFAiEA9eQWGD2KcgiFdw3pUU1l1XJRQ2
/2K4CcNsPsrs8Ns0gCIQCk70SQQpD7hqNffzbZsJCw4hF2DZJRmAT5V4nCyAegfQQgfRJt66Wx7mW2LssKeyE8lb7BXpkog5Kk9yzpbUH
/PSQEW5eHqlPDnuklTz9xkMLWE7dkxpLHGC9e0u53
/VCTeCpPnqH1A3yTrkyI8ASpv9X70JldyHJkmJb0BrBiningTZmL0KAXvGLuWsdqvJUOikJW5QvSPI/HlO0vDC4="
  }
}
```

操作结果

如果调用中某一步服务端认为过程出错，将返回以下结构给浏览器：

```
 {
  "type": "http_response",
  "content": {
    "code": "xxx" // "SUCCESS"
  }
}
```

如果返回的code不是SUCCESS，服务端将主动**断开websocket连接**

在最后一步，即浏览器将ukey结果转交给服务端后，在服务端返回以上结构给浏览器后，服务端将主动**断开websocket连接**：