|  |
| --- |
| **围炉送温暖 Fireside Help (v0.4 2020.4.5)**  2020.1.23，中国武汉封城。两个月以后，2020.3.23，美国俄亥俄州宣布宅家令，最初计划到4月6号，后来根据联邦的建议延长到5月1号。很多人在这段时间里失去收入，需要帮助。很多热心人想要帮助这些有实际需要的人，并为没有口罩的人们提供口罩等个人防护用品(PPE)。为此我们设计了一种高效、尽可能保护受助人和捐助人隐私的直捐协议(protocol)。  这个直捐协议有几个目标。第一、保护受助者和捐助人的隐私，维护受助者自尊。只有几个相关的志愿调查者和直接捐助人知道受助者和捐助人是谁，别的志愿者和系统管理员都不知道，更不会公开。第二、捐款是直捐，直接从捐款人打给受助者，不经过第三方。  这个直捐间的协议具体步骤如下：  一、申请人或推荐人准备一些简单信息，包括申请人姓名，联系方式，学校名字（可选），班主任联系方式（可选），父母工作类型和联系方式（可选）等。重点是这些信息不提交系统，申请人只需要提交这些信息的一个验证码SHA1或MD5 hash value。  二、系统为每一个申请人自动匹配一个志愿验证者，因为申请人无法指定验证人，所以申请人不容易作弊。（系统还未实现，现在是人工匹配、指定。）申请人把具体的申请信息，直接发给验证者，验证者通过各种途径验证之后，在系统里提交验证结果。验证结果仅为通过或不通过，不包含任何申请人具体信息。  三、志愿捐助人可以选择一个经过验证的实需生申请人，向验证人索取二维支付码并直接捐款给受助人。然后捐助人发送付款凭证给验证人。验证人在系统里记录该实需生已得到帮助，同时销毁验证人之前收到的实需生信息，为实需生保密。  Separately, donors can also register commitments in the system before a suitable recipient is identified. A verifier will check if the commitment is reasonable. After that, an applicant with matching needs can apply directly to that commitment through the volunteer verifier.  所有公开信息都记录在：<https://lisasiliu.github.io/FiresideScienceChat/Donations>  此网页在微信中打不开，要在浏览器中打开。 |

|  |  |  |
| --- | --- | --- |
| **申请救助** | | |
| 申请人Applicant | 受助条件 | 系统不设具体受助条件。公开的“受疫情影响”描述是捐款人决定捐助与否的关键。  可以由学校老师、社区志愿人员、邻居或者其他推荐人在申请人同意的情况下代为申请。  *\*\* 申请人或家人有没有被新冠病毒感染与此申请无关，关键看受疫情影响。* |
| **公开信息**  （这些信息会被永久保存） | 1. 申请人信息的验证码（SHA1 或MD5） 2. 地区（用于验证人选择）(如湖北武汉，或湖北汉口) 3. 受疫情影响（具体回答可以帮助捐助人做决定） 4. 收款方式或收款二维码的验证码 |
| 申请人信息 （仅验证人 和捐助人可见，不公开） | 1. 姓名和联系方式 2. （可选）学校/班级 3. （可选）班主任姓名和联系方式 4. （可选）推荐人姓名和联系方式；推荐理由 5. （可选）父母姓名、工作、联系方式 6. 收款二维码 |
| **志愿验证** | | |
| 验证与协调人  Verifier and coordinator | 验证任务 | * 验证人要明确判断申请人符合条件否以及申请人信息可信否。 * 验证人要提供地区信息以方便系统配对。 * 验证人负责生成实需生防重码，以防同一申请人重复进入系统。防重码根据申请人姓名地址或学校班级（无标点符号，无空格，无阿拉伯数字）生成。系统永久记录实需生防重码，但不记录申请人其它信息。 * 验证人还负责把收款二维码发给志愿捐助人。 * 最后验证人把捐助人的实名、匿名、或笔名更新到公开信息中。 * 验证人同意为申请人和捐助人保密，捐助完成后删除相关信息。 |
| **志愿捐助** | | |
| 捐助人  Donor | 捐助现有申请人流程 | 捐助人自愿选择一个已验证过的实需生，联系验证人，获得收款二维码，用公开的收款二维码的验证码验证收款二维码，直捐，发捐款截屏给验证人。  捐助人可以实名、匿名、或用一个笔名。 |
| 捐助人发起流程 | Donor commits to a specific amount of funds or goods or a particular service. Send checksum of the info to the system. The system assigns a verifier to ensure the pledge is reasonable. Later, a verified applicant can be matched with a committed donor to complete the transaction. |

|  |  |  |
| --- | --- | --- |
| **Donor commitments** | | |
| Committed Donor | Public Information | 1. Commitment (e.g. $100 or 20 facial masks) 2. Checksum of all other donor information. |
|  | Private Information (only visible to the assigned verifiers) | 1. Contact info 2. Name or pseudo name 3. Reasonable description/proof/evidence of the commitment |

**注意：**微信发送收款二维码图片时，即使是原图发送，也会被压缩。为保证验证码能成功，请用zip把二维码图片打包后再传送。

SHA1 或MD5 都是成熟的开源算法，其验证码可以用以下几种方式或其它工具生成。

* <http://onlinemd5.com/> 国外可访问
* http://tools.jb51.net/password/sha1encode 只能为文本生成MD5码
* Android App：Hash大师,HashStamp MD5 & SHA1 Checker等
* Mac上自带sha1和md5软件

MacBook-Pro:Desktop changliu$ which md5

/sbin/md5

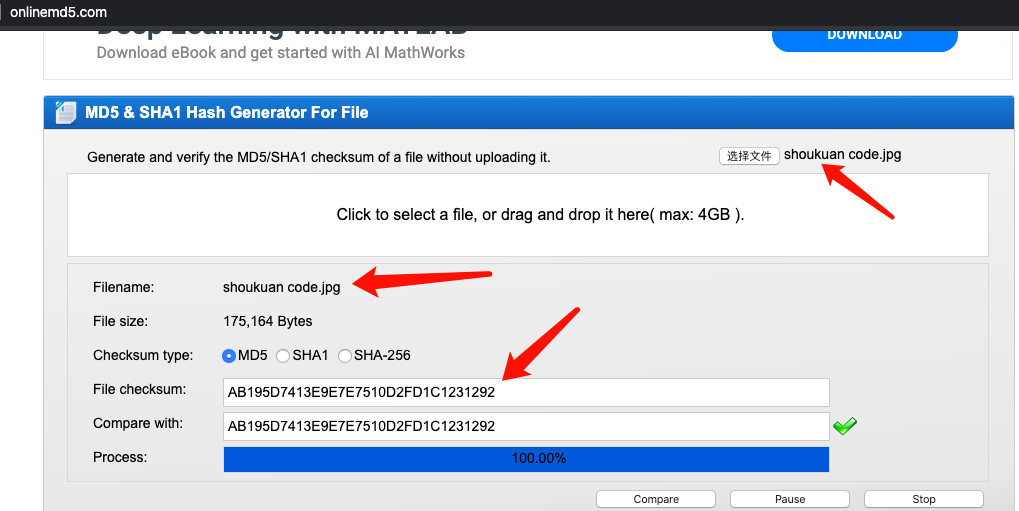
MacBook-Pro:Desktop changliu$ md5 shoukuan\ code.jpg

MD5 (shoukuan\ code.jpg) = ab195d7413e9e7e7510d2fd1c1231292

MacBook-Pro:Desktop changliu$ openssl sha1 shoukuan\ code.jpg

SHA1(shoukuan code.jpg)= ff4d4d0f61160755bde11ada717e887ed1fc3bf8

* 这一篇文章讲怎样用WINDOWS或LINUX自带的工具进行校验，供参考<https://jingyan.baidu.com/article/fec4bce21f08bdb2618d8bcc.html>



不熟悉验证码的人可以直接联系刘畅，我们可以帮助你们完成申请。

**** 请注明“围炉送温暖”，谢谢。

**围炉送温暖 Fireside Help**

**实例：实需生Student-in-need 001**

**围炉送温暖申请人公开信息 （2020.3.14）**

|  |  |
| --- | --- |
| 实需生信息Word Doc文件MD5校验码 | 628c73df76c15dd8a6431a8b784f4459 |
| 地区 | 湖北武汉 |
| 受疫情影响（可选） | 父亲病逝由母亲抚养，母亲务农，家庭经济困难。 |
| 收款二维码JPG图片的MD5校验码 | ab195d7413e9e7e7510d2fd1c1231292 |

**围炉送温暖申请人信息**（仅验证人和捐助人可见，不公开）

1.姓名：XXX 联系方式：111111111111

2.学校：武汉XXXXX学校 XXX二班

3.班主任姓名/联系方式：XXX 11111111111

4.母亲姓名：xxxxx 工作：xxxxx 联系方式：1111111111

5.推荐人姓名：XXXX 联系方式：11111111 推荐理由：XXXXXXXXXXXXX。

**验证人生成信息**

防重码：XXXXXXXXXXXXXXXXXXXXXXXXXX（实需生姓名学校班级）

9377BD31C6D279BE299BC87F6BCA5C17 (MD5)

**捐助人信息**

围炉800元 + prana 200元 = 共 1000元 （2020.3.14）

所有公开信息都记录在：<https://lisasiliu.github.io/FiresideScienceChat/Donations> 此网页在微信中打不开，要在浏览器中打开。