Annex A

Terms of Reference (TORs)

Exploring Blockchain or other appropriate Technology Options in Support of a Trust Scheme for Refugees consisting of a

- **Self-managed Digital Wallet for Individual Refugees**
- **Document Verification Registers (e-Registry and e-Apostille)**

United Nations High Commissioner for Refugees,

Geneva (Switzerland)

Table of Contents

1 Introduction

1.1 Overview and objectives of the Terms of Reference

UNHCR wishes to appoint a supplier (including consortia) to implement Blockchain or other appropriate Technology Options in Support of a Trust Scheme for Refugees (hereinafter referred to as "the System") that will enable a) Self-managed Digital Wallet for Individual Refugees and b) Document Verification Registers (e-Registry and e-Apostille) of Persons of Concern (hereinafter referred to as PoCs) in UNHCR operations globally.

UNHCR is looking to appoint a supplier (including consortia) who is experienced in implementing Blockchain or other appropriate Technology Options in Support of a Trust Scheme in diverse locations and who will be sensitive to the varied work of the organization. The proposal should consider suitable technology options (particularly blockchain distributed ledgers, but also other appropriate technologies) and have three distinct but interrelated components:

- Self-managed Digital Wallet for individual refugees
- Certified Record of Action (e-Registry)
- Digital certificate of authentication (e-Apostille)

The scope of the proposal is explained in detail below. However, it is meant to be a pilot and proof of concept project using real data from selected UNHCR operations.

The requirements catalogue contained in this RFP details the functional, IT and non-functional requirements for the System as well as describing the key business processes, quality requirements, the core functionality requirements, as well as the technological environment and requirements for the new System.

Political, regulatory and reputational aspects are not in the focus of this proposal. Instead, submissions should concentrate on technical and business/organizational aspects.

UNHCR will invite bidders to a **public Pitching Event in the last week of November 2018 (planned date: 27 November) in Copenhagen.** The Pitching Event will give bidders the opportunity to present their approach and engage in a dialogue with representatives of UNHCR before handing in their full proposals. Interested bidders are encouraged to participate in the Pitching event. Participation in the Pitching Event is not mandatory to hand in a proposal, it is, however, recommended to participate in this supplier conference. To ensure that all potential bidders have access to the same information, the conference will be recorded and available online until the RFP deadline. The recording will also include all questions put forward by participants at the Pitching event conference and the answers provided by UNHCR as well as any additional information which will then be shared publicly with all potential bidders. Please note that no discussion on financial proposal will be allowed at the event.

The Pitch will not be part of the formal evaluation of the proposal.

The deadline for submission of questions that will be addressed at the pitching event is **November 22, 2018**. The closing date for offers submission is 18 January 2019. **A contract in form of a frame agreement will be awarded immediately upon completion of the evaluation.** The project implementation is foreseen for 2019. For an overview of the tender process please refer to Annex 5.

Fraunhofer Gesellschaft (FHG) will assist UNHCR in the analysis of the proposals received and representatives of FHG will be present at the Pitching Event.

UNHCR has a well-defined procurement process. The evaluation of bids will be done by a joint team of business, IT and procurement professionals. Information on the structure of the replies and the methodology for scoring and short-listing of bids can be found in Annex 5 of this RFP. These documents also contain a general overview of the process and steps that UNHCR will take before awarding a contract to the successful bidder.

Overall success of the project will be defined by meeting the functional, non-functional and technical requirements as laid out in the document alongside offering value of money. However, the ultimate success of the System will be determined by the willingness of UNHCR field operations to utilize the System and therefore the System must at all times be designed with the needs of these users and the environments in which they work.

The structure of this document is as follows: In an introductory chapter, there is a short introduction on the legal basis and processes of identity management by UNHCR. The chapter will dwell on the High Commissioner's vision to use data for the empowerment of the individual and the need to develop UNHCR into a Trust Authority for that purpose. In the second chapter, use cases will be discussed and the project statement presented.

In the third chapter, we explain the operational context, in particular the intention to establish a UNHCR Trust Scheme in full accordance with the organization's Policy on the Protection of Personal Data of Persons of Concern. Hence, the ultimate goal to design a system of self-managed digital wallets for asylum seekers, refugees, stateless and other forcibly displaced persons. While the submissions under this Request for Proposals must be in line with UNHCR's protection mandate, privacy policy, control through system design, safeguarding data privacy, security and user rights, proposals on an accompanying comprehensive legal and regulatory framework are not required.

There are several annexes elaborating the elements of the planned Trust Scheme and a Glossary providing some background information on the terms and measures used in the text.

2 Identity Management and Registration in UNHCR Operations

In modern society, individuals require an identity as a necessary pre-requisite for the enjoyment of all civil and political rights, access to services, and socio-economic inclusion. The empowerment of asylum seekers, refugees, and other forcibly displaced persons is the primary objective for UNHCR's role in identity management.

Registration is the recording, verifying, and updating of information of refugees and other forcibly displaced persons in order to facilitate UNHCR's work of protecting, documenting and assisting them.

The involvement of UNHCR in both identity management and registration requires careful co-ordination with Governments. Article 16 of the International Covenant on Civil and Political Rights (1966) stipulates that everyone shall have the right to recognition everywhere as a person before the law. More specifically, Article 25 of the 1951 Convention Relating to the Status of Refugees confers the obligation to each country of asylum to deliver to refugees identity documents or certifications1. In legal theory and practice, the prerogative of the States is to ensure a system that guarantees the establishment of legal identities and the issuance of foundational documents (tokens), such as birth certificates, ID Cards (also called a piece of identification or ID, or colloquially as papers), passports so that an individual may use it to prove his/her identity.

As part of the Sustainable Development Goals (SDGs), the United Nations General Assembly in September 2015 endorsed goal 16 which aims to provide legal identity for all, including birth registration (target 16.9). All nations and UN agencies are committed to achieving this goal by 2030, thereby addressing the contemporary problem of the more than 1 billion persons globally with no personal identity document. Some of them are asylum seekers, refugees, stateless and forcibly displaced persons.

The inclusion of target 16.9 means that the provision of legal documentation is being recognized and addressed as a global development issue. As the most viable way to implement this target, the UN agencies and Bretton Woods institutions regard the establishment of integrated population registries that include the entire population living on a State's territory, regardless of nationality, or legal status. Hence, UNHCR advocates for the inclusion of asylum seekers, refugees, but also stateless persons, and other forcibly displaced persons into such unified registries.

There are different types of identity. The most powerful is a legal identity that empowers the individual to fully participate in the life of a community with all rights and no restrictions. However, there are sub-sets of identities which are equally important. In particular, if refugees should be denied a fully-fledged legal identity, such as an economic identity to engage in commercial transactions, a digital identity to access the internet, and on-line services, such as in education and health care.

UNHCR's involvement in identity management, including registration, aims at establishing (where needed) or strengthening identities according to internationally accepted standards, procedures and trust frameworks. The objective is not to prevent the refugees from becoming victims of identity theft or remaining in other ways invisible, but to contribute to the empowerment of the individual and give him/her power over his/her identity data.

[1] Article 25 of the 1951 Convention Relating to the Status of Refugees authorizes an international authority to arrange for administrative assistance "to refugees such documents or certifications as would normally be delivered to aliens by or through their national authorities … Documents or certifications so delivered shall … shall be given credence in the absence of proof to the contrary." Hence, the extend and limits of UNHCR's engagement are set-out in international law, incl. the Conclusion on Registration of Refugees and Asylum-seekers No. 91 (LII) – 2001, by UNHCR's Executive Committee as well in bilateral agreements between UNHCR and national governments.

Civil registration by States is defined as a system to record vital events (births, marriages, and deaths) of citizens and residents. Here, the primary purpose of civil registration is the creation of legal documents that can be used to establish and protect the rights of individuals. Another purpose is to create a data source for the compilation of vital statistics. UNHCR may be asked by States to undertake certain registration activities in support of the State's registration functions. The further development of a Trust Scheme whereby UNHCR acts as a trusted (electronic) identity provider.

- Reassures Governments that identities and documents carried by refugees are certified according to international standards and are, thus, trustworthy.
- Provides individual refugees with identities and documents that are useful to them because they will be recognized by State authorities and businesses.

While registration focus on the individual, providing a unique individual identity to each person, UNHCR and States have a responsibility to maintain family unity and to re-establish family unity where it is lost. An important objective of identity management is to document family composition for reasons relating to status, access to rights and services. Accurate registration of children helps to prevent military recruitment, child labour and trafficking. Durable solutions also require the correct registration and documentation of both individuals and families.

UNHCR Field colleagues are often faced with individuals unable to present proper identification documents. Neither can families always present UNHCR with State-issued documents confirming the family composition. In these cases we speak of "claimed identities". No UNHCR official is expected to apply forensic sciences and to investigate, by whatever legal standards, individual and group identities during the registration process. Simple evidence and plausibility rules (appearance, language, etc.) apply. Fixing a population, i.e. ensuring that everybody is enrolled at least but never more than once, is sufficient for managing basic protection and assistance activities, in particular in mass displacement situations.

Over time, and in particular for important use cases, e.g. when an individual applies for a tertiary education scholarship, the collection, preservation, and analysis of evidence might be required. Identity proofing is an important prerequisite for the establishment of confidence and trust assurance levels. It is obvious that UNHCR cannot assign the same trust level to somebody with a "proof of registration card" who has not provided any identity token, as against somebody who has obtained his/her "Refugee ID Card" on the basis of evidence and credentials presented and RSD interviews conducted.

The increased transfer of assistance services to the internet, however, requires reliable identification and authentication systems, in line with the Policy on the Protection of Personal Data of Persons of Concern[2]. Identity Management is the key activity that brings UNHCR close to the people it is mandated to protect and assist. Registration is often the first and most critical step in a journey that starts with forced displacement and ideally ends with a solution to flight and asylum.

[2] See: www.refworld.org/pdfid/55643c1d4.pdf

3 Overview on Use Case and Project Statement

3.1 Access of Data Subjects to their Data

The business case put forward is the use of suitable technology options (e.g. blockchain distributed ledgers) to strengthen the identity of refugees (data subject) who will obtain certified documents and have agency over those in a self-managed digital wallet. Currently, UNHCR holds identity records of more than 8 million refugees globally. UNHCR's Population Registration and Population Management EcoSystem (PRIMES) records the bio data (or foundational data), such as names, birth date, nationality, place of residence, but also a passport size picture and biometric imprints. None of these data elements is currently accessible, neither in parts nor in total) to the data subject.

While the current system records status, e.g. somebody being married or holding a degree or diploma, these supporting documents are not uploaded into the system. Likewise, the documents produced by the system, such as ID cards, family attestations, are printed on paper and handed out to the individual. There are no digital records maintained in PRIMES.

As an eco system, certain PRIMES applications support UNHCR management activities, for example CashAssist (cash payments) and GDT (commodity distribution). As UNHCR intends to develop a specific application for the management of currently more than 6,700 students in 50 countries that receive tertiary education grants (DAFI)[3], the project outlined here, will be of specific significance: refugees that apply for scholarships and those that are awarded scholarships will be part of the pilot group managing their own digital wallets.

3.2 Enabling Self-Management of Data by Providing Trust Services

The High Commissioner has expressed his vision that every refugee should have his unique digital identity[4]. For a digital identity to be practical and useful, it has to be recognized by other main actors in our societies: authorities, institutions of higher learning, businesses. A recognized identity empowers the individual and is an enabler for socio-economic inclusion.

In the identity model put forward by UNHCR, the individual refugee has agency over and should be managing his/her identity, while UNHCR puts its institutional weight behind the individual identity.

The document verification registers (e-Registry and e-Apostille) will emulate the traditional apostille system[5] used by States and authorities to authenticate the origin of public documents to be used in another jurisdiction. Blockchain distributed ledgers (or other appropriate technologies) would host the e-Registry consisting of Certified Records of Action relating to all data of UNHCR data subjects, such as individual asylum seekers, refugees stateless and other forcibly displaced persons. Each such meta data record would confirm the action taken without disclosing the person, the substance of the action or the data.

An e-Apostille would contain more data, in particular data that allows to link the data to a specific person. Hence, an e-Apostille, even though it might have been generated in an automated manner, will therefore be moved into the digital wallet and be managed by the data subject himself. That would allow individual asylum seekers, refugees stateless and other forcibly displaced persons to store and, if the need arises, to share both the digital document as well as the e-Apostille with governmental authorities, institutions of

[3] See: http://www.unhcr.org/blogs/new-digital-solutions-refugees-education/

[4] See www.refworld.org/pdfid/55643c1d4.pdf

[5] www.loc.gov/law/foreign-news/article/international-electronic-apostille-program-developments/

higher education, and businesses that require these documents for establishing an identity, authentication, or any other relevant process.

Public documents frequently need to be used across borders – especially in the case of asylum seekers and refugees who – by definition – are outside of their country of origin or habitual residence. Before one can use such documents in another country, their origin must be authenticated. The traditional method employed by States that are not members of the Apostille Convention is called legalization and is often a slow and costly process. (Contracting States to the Apostille Convention agreed to reduce the authentication process to a single formality — issuance of a certificate of authentication (apostille) by a competent local authority, depending on the nature of the public document involved [6].

The digitalization of public services and the introduction of e-Governance has brought about the introduction of an electronic Apostille Program (e-APP) by some States. These States, all of them HCCH member States7, thereby implement an e-Registry and/or an electronic Apostille programme (e-APP).

E-Registries contain Certified Records of Action that are accessible online and enable the recipients to readily verify the origin of a document (with apostille) they have received.

Information in e-Registries is stored securely. Security measures employed by the concerned States to date include provision of a URL with a unique identifier, the use of a Quick Response (QR) code and of SSL [Secure Sockets Layer] Certificate or similar technology, for third-party verification. Users of e-Registries also may be prompted to enter a randomly generated word to ensure that the user accessing the information is not a computer.

Over 200 competent authorities from 29 Contracting States have to date implemented components of an **electronic Apostille programme (e-APP)** promoting the use of electronic apostilles that can be shared online by UNHCR data subjects with any recipient and which verify the origin and the legitimacy of the apostille.

Normally, an e-Apostille is a digitally signed electronic file that is transmitted by electronic means, such as e-mail, or is made available otherwise for download or viewing from a website. This electronic file contains an electronic apostille certificate attached to either an original electronic public document or a paper document that has been previously scanned.

Benefits of the use of an e-Apostille include non-expiration of e-Apostilles, which continue to be valid even after the digital certificate of the person signing the e-Apostille expires; an easy and secure method of attaching apostilles to the underlying public document, as required by the Convention; and a decrease in the possibility of fraud associated with the attachment of traditional paper apostilles. In addition to combatting fraud and reducing the operational costs associated with paper apostilles, e-Apostilles can be freely used with paper public documents that are subsequently scanned and digitized. This brings the Apostille Convention in tune with the growing trend among government authorities to execute and make public documents available in electronic format.

3.3 Blockchain distributed ledgers (or other appropriate technologies), DAFI and the proposed UNHCR Trust Scheme

Operating a trust scheme would enable UNHCR to define the organizational, technical and regulatory/legal rules, which the entities have to fulfil. These rules and trust policies are defined centrally

[6] Apostille Handbook - A Handbook on the practical operation of the Apostille Convention (2013), at xviii, website of the Hague Conference on Private International Law www.hcch.net/en/home

[7] These countries developing e-Registries and e-Apostilles are listed here: https://assets.hcch.net/docs/b697a1f1-13be-47a0-ab7e-96fcb750ed29.pdf

and are valid for all enrolled entities in this trust scheme. In a first phase covered by this pilot this are likely to be UNHCR internal entities, public notaries, and institutions of higher education.

The Trust Scheme enables UNHCR to decentralize the processing (e.g. digitalization process), initially of DAFI relevant documents only. However, DAFI applicants do not only need academic credentials but documents relating to

Their status as refugee

On family relationships since only one scholarship is assigned per family

The economic situation of the applicant

There will be lists of trusted third parties, which digitize and verify documents and upload them into the UNHCR Trust scheme. If the pilot is successful, other potential trust service providers, such as other programs of the United Nations (World Food Program, Unicef), will be invited to join, thereby contributing to strengthened identities of refugees as well as to the digitalization and transformation process for UNHCR.

In the first phase it is unlikely that a system of "Levels of Assurance (LoA)", based on a scoring system such as used by eIDAS or NIST8, will be implemented. Once this happens, in addition to the trust scheme membership, the degree of confidence into the participating entity can be considered.

3.4 Architecture and Transactions within the Trust Scheme

The architecture of the Trust Scheme is based on decentralized data bases for which the participation entities are responsible, including the digital wallet managed by the data subject. However, the blockchain distributed ledger (or other appropriate technology) based e-Registry will store records on all identity relevant transactions. So-called Certified Records of Action (CRoA) stored in the e-Registry would not disclose any personal information on the data subject. The information on this record/register is restricted to meta and process data showing that the digitalized information is genuine and has been generated as part of the UNHCR Trust Scheme. Each CRoA would be generated in an automated manner as would be the e-Apostille. This digital certificate provides the meta data for a single action (e.g. biometric registration) or a document (e.g. digitalization of a paper document) under the Trust Scheme. Like its analogous predecessor, an e-Apostille is intended to legalize a document for use in another country or another authority. Traditionally, the apostille confirms that a government form, signature, seal or stamp on a document is genuine.

The e-Apostille is stored where the respective document is held, i.e. in the digital wallet of the data subject and in the data base of the issuing Trust Scheme entity.

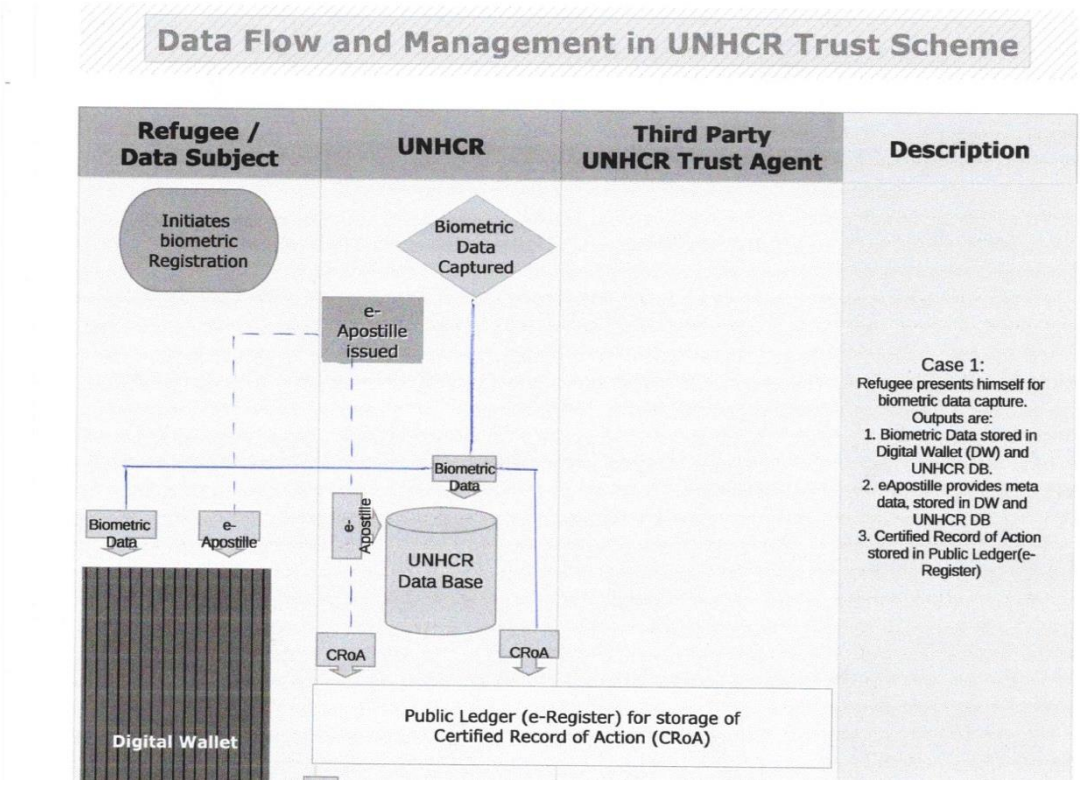
In view of the foregoing, the submissions under this Request for Proposals, proposing a planned Document Verification Register (e-Registry and e-Apostille) as part of the UNHCR Trust Scheme, should use Blockchain distributed ledgers (or other appropriate technologies) for storage of Certified Records of Action (CRoA) in the e-Registry. The following digital transactions (list is not exhaustive) would generate CRoA to be stored and made accessible in the e-Registry:

- Biometric registration conducted
- Individual ID document issued
- Family Attestation issued
- New digital document established
- LoA score issued
- Validity of previously issued document extended

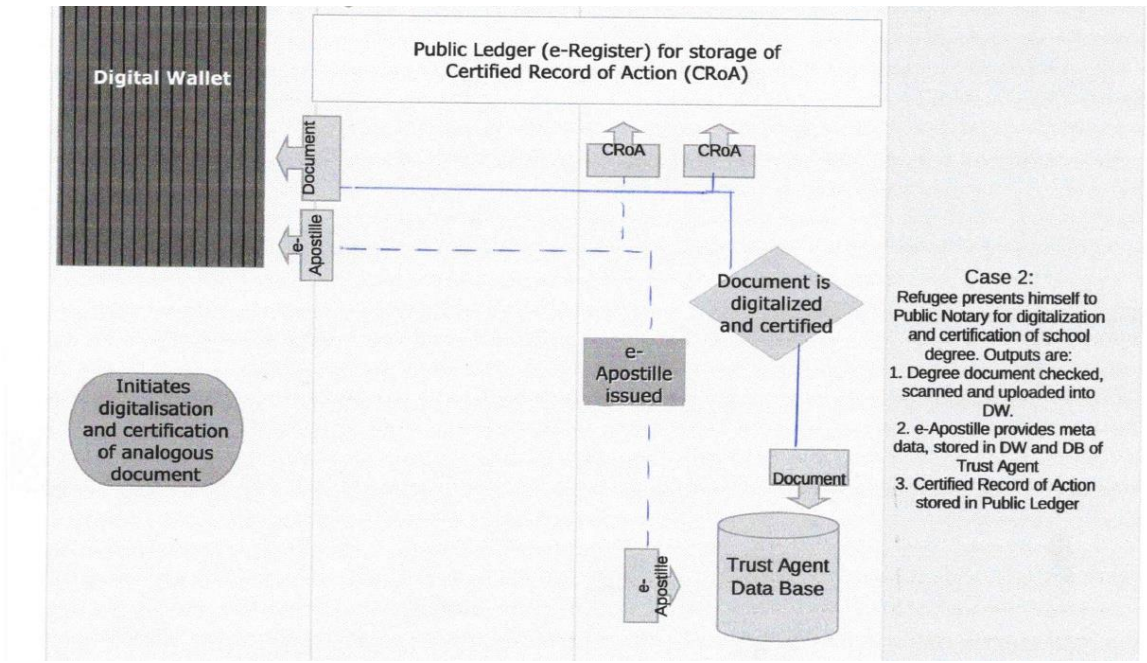
[8] NIST is the National Institute of Standards and Technology and, as a physical sciences laboratory, a non-regulatory agency of the US Department of Commerce. https://pages.nist.gov/800-63-3/sp800-63-3.html

- Validity of previously issued document revoked
- Already existing paper document verified
- Already existing paper document digitized and uploaded
- Digital signature issued
- Digital delivery / reception confirmed

In the following example the data flow is described for the case of the capture of biometrics:



In the second example a refugee requests a UNHCR Trust Entity/Agent, such as a public notary, to verify an academic record and to digitalize it for his/her digital wallet:



The pilot project will deal with a very limited number of data subjects only. However, as candidates and recipients of scholarships they have major certification needs. The project will identify a limited and clearly defined types of applications for generating, storing, and accessing CRoA and e-Apostilles. Not all aspects of the project might require blockchain distributed ledger technology (if blockchain distributed ledger technology is required at all). The Digital Wallet is outside the scope of a public distributed ledger / blockchain given the highly sensitive nature of the identity documents of our caseload.

Hence, it is also conceivable to deploy blockchain distributed ledger technology in a complementary fashion with other technological solutions. Blockchain distributed ledgers should only be deployed where it provides value in practice, is cost effective, and technologically superior to any other technology.

Should the pilot project fail to deliver, the risk remains manageable given the limited number of application and use cases. While the project would take off, paper-based process currently used would still exist in parallel. Moreover, no tracible document on a UNHCR data subject will be stored in the public blockchain / distributed ledger, so that the privacy risks are limited.

The blockchain / distributed ledger could be either public (e.g. based on Ethereum) or private (shared among UNHCR and participating trust scheme entities). The decision on whether a public or a private blockchain / distributed ledger should be used (if at all) depends on various details of the pilot. At this stage, UNHCR believes that in the context of the use cases presented in this document, both options are viable and could make sense. If a public distributed ledger is used, privacy aspects will have to be closely considered – even if only metadata is stored there.

For the use cases under discussion, only a very limited amount of information will need to be stored on the blockchain distributed ledger. Hence, transaction throughput and costs are manageable. Transaction throughput is only limited when storing a new e-Apostille on the blockchain distributed ledger for which case also costs might incur.

3.5 Policy on the Protection of Personal Data of Persons of Concern to UNHCR and Privacy by Design and Default

Data protection is a longstanding priority for UNHCR. In the Policy on the Protection of Persons of Concern to UNHCR, promulgated in May 20159 terminology and practices have been aligned closer to general principles and concepts of data protection, such as the GDPR adopted by the European Union. UNHCR is a very data intensive organization keeping records of more than 8 million individuals globally. UNHCR staff and colleagues in partner organizations need to process daily a lot of information on individual refugees, asylum-seekers, internally displaced persons, and other people whom the organization protects and assists.

The Policy was adopted for a more principled approach and the acknowledgment of certain rights refugees have as data subjects. The organization's data protection policy demands privacy and control through system design and aims at safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.

UNHCR, having endorsed the 2018 Principles on identification for sustainable development10, has committed to further principles, such as proportionality and minimal disclosure, incl. that authentication and other protocols should only disclose the minimal data necessary to ensure appropriate levels of assurance. Identification systems—including credentials and numbering systems—should not disclose sensitive personal information.

By adopting the principle of Privacy by design and by default, UNHCR will put in place all appropriate technical and organizational measures to implement data protection principles and safeguard individual rights. Where this is not yet the case, UNHCR will embark on retro-fitting.

In essence and for the purposes of the pilot project of this RFP, data protection and privacy are absolutely essential and ought to be given highest priority when processing activities and business practices, from the design stage right through the lifecycle.

[9] See www.refworld.org/pdfid/55643c1d4.pdf

[10] World Bank. 2018. Principles on identification for sustainable development: toward the digital age. Washington, D.C. : World Bank Group http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-identification-for-sustainable-development-toward-the-digital-age

Annex 1

The DAFI Programme

The DAFI programme (Albert Einstein German Academic Refugee Initiative) plays an integral role in enabling refugees worldwide to access higher education. Undergraduate refugee students are provided with scholarships that cover a wide range of costs, from tuition fees and study materials, to food, transport, accommodation and other allowances.

Access to higher education motivates refugee children to stay in school and succeed academically. For students and graduates, the DAFI programme serves as a foundation for social and professional development, allowing them to build careers in competitive fields of employment. The social returns of the DAFI programme exceed investment at the individual level. Highly educated refugees reduce economic and psychological dependence, improving their self-reliance and offering long-term solutions.

- The strategic priorities of the DAFI programme are to:Promote self-reliance of sponsored students through opportunities for employment and entrepreneurship;
- Empower students to contribute knowledge, skills and leadership to the refugee community, and to facilitate peaceful coexistence with host communities during displacement;
- Strengthen the protective impact of education by encouraging lifelong learning for young refugees;
- Foster future role models for refugee children and youth to demonstrate the impact of education on individuals, communities and societies.

A lack of a legally recognized identity prevents people from exercising their fundamental rights. Identity is essential for a life in the modern world: to access services or a scholarship and to attending a tertiary education is the dream of many refugees.

Also, the Sustainable Development Goal No. 4 seeks quality education and lifelong learning opportunities while SDG No. 16.9 is about providing a legal identity for all.

Since 1992, through the dedicated support of the German Government and private donors, the DAFI programme has supported over 14,000 young refugees by giving them the opportunity for increased self-reliance through the acquisition of knowledge and skills and subsequently to gain employment to support their communities. In 2017, over 6,700 students in 50 countries benefitted from a DAFI scholarship, including over 2,582 newly enrolled students. 41% of DAFI scholars in 2017 were female.

The identification and selection of candidates to obtain a DAFI scholarship is resource and time intensive and requires further digitization to increase its efficiency.

At present, refugees applying for DAFI scholarships are reliant on the ad hoc recognition of UNHCR identity documents as well as certificates of educational institutions. Disbursement of scholarship funds may also be impacted by regulated 'know your customer' requirements for identity recognition by banks, and the ability of the scholar to have his or her degree recognized following completion of the course may also be limited subject to the individual's ability to assert their identity.

By exploring blockchain distributed ledger (or other appropriate technology) options in support of a Trust Scheme for refugees consisting of a self-managed Digital Wallet for individual refugees and document verification registers (e-Registry and e-Apostille) UNHCR seeks to intensify its establishment of a trust scheme including the setting of a recognized identity standard by which persons of concern can apply easier for the UNHCR distributed DAFI scholarships.

Annex 2

Key Elements of a proposed UNHCR Trust Scheme[11]

A. Relevant Definitions

Trust Scheme
A Trust Scheme is operated by a Trust Scheme Authority and comprises the organizational, regulatory/legal, and technical measures to assert trust-relevant attributes about enrolled Entities in a given domain of trust. A Trust Scheme operates in a given Trust Domain and typically has a declared or implied purpose.

Entity
An Entity is a person, organization, or thing that is enrolled in a Trust Scheme and certain attributes of which are certified by a Trust Scheme Authority.

Trust Scheme Publication
A Trust Scheme Publication is always associated with a Trust List which indicates that an Entity operates under the Trust Scheme, which the Trust Scheme Publication corresponds to. Trust Scheme Publication is always operated by a Trust Scheme Provider.

There are different types of Trust Scheme Publication. Boolean Trust Scheme Publications indicate the entities that comply with the requirements of the trust scheme, and thus are a member of the trust scheme. Ordinal Trust Scheme Publications indicates the entities that comply with the requirements of an ordinal aspect (typically, this is a Level of Assurance (LoA)) of the trust scheme.

Trust List
A Trust List is a specific data file of a specific format that is certified by the issuing authority (e.g., via electronic signature). It provides a list of all the enrolled entities. Trust Lists can be associated with a Boolean or Ordinal Trust Scheme Publication.

An existing and widely accepted standard for trust lists is ETSI TS 119 612 (ETSI TS 119 612, V2.1.1 (2015-07), 2015).

Trust Scheme Provider
A Trust Scheme Provider operates a Trust Scheme. It decides, whether an Entity is associated with its Trust Scheme. The Trust Scheme Provider provides the Trust Lists for a Trust Scheme.

B. Example of an existing, international Trust Scheme

One prominent example of existing Trust Schemes is eIDAS in the European Union. The eIDAS Regulation (Regulation (EU) N°910/2014) on electronic identification and trust services for electronic transactions in the internal market provides a regulatory environment for electronic identification and trust services, including electronic signatures, seals, timestamps, registered delivery and website authentication.

In there "Trusted Lists are essential elements in the building of trust among market operators as they indicate the qualified status of the service provider at the time of supervision"[12]. For the qualified status different assurance levels can be assigned, e.g. for electronic identification the assurance levels are low, substantial, and high.

[11] This Annex has been developed by the LIGHTest project as part of its collaboration with UNHCR.

[12] As an example for eIDAS Trust Service Status Lists, the Trust Service Status List of Germany can be downloaded from https://www.nrca-ds.de/st/TSL-XML.xml.

UNHCR would define the requirements for information processes, processes for issuance or revocation, requirements towards used technologies, or simply single one-dimensional requirements (e.g. the geographical location of an entity). As the UNHCR Trust Scheme does not yet exist, the following points need to still to be designed: trust scheme policy, trust scheme membership, trust anchor, and requirements.

C. Trust Scheme Policy

The set of requirements is part of the Trust Scheme Policy. Following, ETSI TS 119 612, the trust scheme policy is specified as part of the Scheme information section in the overall structure of trusted lists. Hereby, several tags provide information on the trust scheme policy.

The tag <SchemeTypeCommunityRules> "specifies the URI(s) where users (relying parties) can obtain scheme type/community/rules information against which services included in the list are approved and assessed, and from which the type of scheme or community may be determined." Among other things "The referenced URI(s) shall identify (i) the specific policy/rules against which services included in the list are approved and assessed, and from which the type of scheme or community may be determined; (ii) the description about how to use and interpret the content of the trusted list.".

The tag <PolicyOrLegalNotice> "specifies the scheme's policy or provides a notice concerning the legal status of the scheme or legal requirements met by the scheme for the jurisdiction in which the scheme is established and/or any constraints and conditions under which the TL is maintained and published. ...Any referenced text shall provide information describing the policy under which the Scheme Operator operates or any relevant legal notices with which users of the TL should be aware."

The tag < PointersToOtherTSL> "references any relevant trusted list or any list of trusted lists." It is e.g. mandatory for the trusted lists of the EU Member States and it includes the pointer to the List Of Trusted Lists (LOTL) of the EC and can be also used in the UNHCR Trust Scheme.

D. Trust Scheme Membership

As stated above an entity is a person/organization that is enrolled in a Trust Scheme and that is listed in a trusted list, which corresponds to the trust scheme.

Usually the trust scheme memberships are not stored in one trusted list, but in several trusted lists in particular for larger trust schemes. These trusted lists can be structured in a hierarchical form with different levels.

1. UNHCR (Global)
2. UNHCR (National)
3. Selected Public Notaries
4. Institutions of Higher Education

In this hierarchical structure UNHCR (Global) is the top level. In its trusted list according to ETSI TS 119 612, the trust service provider is listed as one <TrustServiceProvider> in the <TrustServiceProviderList>. National trust service providers would be usually the head office of UNHCR in this country or any other trusted service provider in this country. These national trust service providers maintain again lists of trust services or trust centers, which are members (entities) of the corresponding trust scheme and fulfill the requirements and rules defined in the trust policy. On the next level, different individual trust service providers that comply with the public notary rule of the country in question are listed accordingly. If

required an additional camp level could be added, which provides again trust centers of the corresponding trust scheme, but on a camp instead of national level.

This means that all listed trust service providers in this national or camp list can conduct and support UNHCR in the digitalization and transformation process into the UNHCR trust scheme. This can for example be a national-wide list of notaries and public authorities, which are compliant with the UNHCR trust policy.

This is only one possible option of the hierarchical structure of trust scheme memberships. In addition, trust service providers, which are trusted by other agencies and programs of the United Nations (e.g. World Food Program) or by other institutions can be accepted and added to the list of trust service providers conducting the digitalization and transformation process for UNHCR.

E. Levels of Assurance (LoA):

In addition to the Boolean Trust Scheme Publication, which indicates that the entity (e.g. a notary) complies with the requirements of the UNHCR Trust Scheme, there is also the possibility of Ordinal Trust Scheme Publications. Here, in addition levels of assurances (LoAs) of the trust scheme can be defined, e.g. low, substantial, and high as in eIDAS. For each level, a set of requirements is defined with increasing degree of confidence in the process. Hence, in addition to the trust scheme Membership, a certain LoA can be assigned to the entities, which indicates the confidence of the entity.

For the verification of the authenticity of these trusted lists, the trusted lists are signed using public-key cryptography. In the hierarchical form, there is always a trust anchor required on top. At the trust anchor the key pair needs to be known as correct without further evidence.

The hierarchical structure presented in the above example is just one possible realization for trust scheme memberships. It is intended as basis to develop a suited structure for the UNHCR trust scheme. For example, the number of levels can be easily adjusted according to the framework of UNHCR.

F. Trust Anchor

As mentioned in the previous section, each trust scheme requires a trust anchor, which is known to be correct without further evidence. This is also required for the UNHCR Trust Scheme. It is suggested to establish this trust anchor in the UNHCR Global Service Centre in Copenhagen.

If this Trust Anchor is established, the Trust Scheme Membership of any Trust Service Provider in the hierarchical structure can be found and verified.

G. Requirements

Examples of requirements which are used in existing trust schemes are given in this section. In general, there are three major groups, which need to be considered in this context: credentials, identity and attributes.

From this overall list, the requirements, which are in particular of interest for the UNHCR trust scheme, are given below. These are the requirements for Linkage of Identity Information to the Individual, for Identity Proofing, and for Credential.

For the UNHCR Trust Scheme, only a (small) selection of suited requirements from this overall list of corresponding requirements is needed, which needs to be specified and defined by UNHCR.

Possible Requirements for Linkage of Identity Information to the Individual	***Description***
Knowledge-based	A process that compares personal or private information (i.e., shared secrets) to establish an individual's identity. Examples of information that can be used for knowledge-based confirmation include passwords, personal identification numbers, hint questions, program-specific information and credit or financial information.
Biological or behavioural characteristic confirmation	A process that compares biological (anatomical and physiological) characteristics in order to establish a link to an individual (for example, facial photo comparison).
Trusted referee	A process that relies on a trusted referee to establish a link to an individual. The trusted referee is determined by program-specific criteria. Examples of trusted referee include guarantor, notary and certified agent.
Physical possession confirmation	A process that requires physical possession or presentation of evidence to establish an individual's identity.

Possible Requirements for Identity Proofing	***Description***
Published Identity Proofing Policy	A published identity proofing policy, which must be adhered to, is always required. This is always part of the identity proofing process
Self-Claimed / Self-Asserted	An identifier may be self-claimed or self-asserted.
Policy Compliant Authoritative Document	The policy compliant authoritative document should be identity proofing policy compliant.
In-Person Proofed	In Person Proofing is foreseen for Person Entities
Not-In-Person Proofed	Not-In-Person Proofing is foreseen for Person Entities
Non-Person Entity	Non-Person Entities can be enrolled
Contact Information Verified	Contact Information has to be verified by a third party.
Personal Information Verified	Personal Information has to be verified by a third party.

Entity Secret Verified	Additional secrets of the entity have to be verified.
Verified Credential Claim	The claim of possession of a LoA3 Credential has to be verified.
Entity Information Recorded	Information on Non-Person Entities have to be recorded (e.g. MAC Adress, IP Adress, etc.).

Possible Requirements for Credentials	***Description***
Authoritative Party	An approved, recognized or trusted body that provides assurances (of credential or identity) to relying parties
Credential Binding	Assurance that credential is/remains bound to correct entity
Hardware Security Module	Containment in the credentials against tampering
Credential Broker	Broker for credential service between an individual and an Authoritative Party (Credential Service Party)
Registration Authority	A Registration Authority that provides the credential.
Relying Party Scoped Credential	A credential that allows a user to authenticate itself to the relying party for which the credential was made
Credential Risk	The risk that an individual, organization or device has lost control over the credential that has been issued
Human-Issued	Indicating that a credential has been issued by a human
Network Binding	Indicating that a credential binds a subject to a network
Multi Factor Authentication	Two or more credentials implementing different authentication factors shall be used
Password Strength	Use of strong passwords shall be enforced
Credential Lockout	Lockout mechanism shall be used after a certain number of failed password attempts
Default Account Use	Default account names/passwords shall not be used

Possible Requirements for Credentials	*Description*
Audit and Analyze	Audit trail of failed logins to analyze for patterns of online password guessing attempts
Hashed Password with Salt	Use of hashed passwords with salt
Anti-Counterfeiting	Use of anti-counterfeiting measures on devices holding credentials
Detect Phishing Attacks	Use of practices to detect phishing
Adopt Anti Phishing Practices	Use practices such as disabling images, disabling hyperlinks etc.
Mutual Authentication	Use of mutual authentication mechanisms, e.g. to protect against Man in the Middle (MitM) attacks
No transmit password	Do not transmit passwords over the network (e.g. Kerberos protocol)
Encrypted Authentication	Encrypt data prior to transit if authentication exchange over a network is necessary
Different Authentication Parameter	Use different authentication parameter for each authentication transaction
Timestamp	Timestamp each message with a non-forgeable timestamp
Physical Security	Use physical security mechanisms (i.e., tamper evidence, detection, and response)
Encrypted Session	Protects against session hijacking and man in the middle
Fix Protocol Vulnerabilities	Use platform patches to fix protocol vulnerabilities (e.g., TCP/IP)
Cryptographic Mutual Handshake	Use mutual handshake exchange based on cryptography (e.g., SSL/TLS)
Credential Activation	An activation feature shall be required to use the credential (e.g. entering a PIN into the hardware device containing the credential).
Code Digital Signature	Verify digital signatures against a trusted source to counter the downloading of software that has been modified by unauthorized parties
Liveness Detection	Use liveness detection techniques to identify the use of artificial biometric characteristics (e.g., forged fingerprints).

Annex 3

Detailed Specifications and Technical Requirements

1. Alignment with PRIMES

UNHCR's uses several bespoke software applications, called PRIMES (Population Registration and Identity Management EcoSystem), as its corporate system to manage identities, issue protection relevant ID, and support assistance activities. The major applications are proGres v4 (bio data and case management), BIMS (biometric enrolment), and RApp for off-line registration. PRIMES, holds data of approximately 8 million individuals and is the front-end for more than 2,000 users across the world.

PRIMES is the backbone of many UNHCR operations. The current ecosystem supports the UNHCR business processes as they are defined today: registration, refugee status determination, assistance provision, and de-activation once the refugee status is no longer necessary.

The transformation of a single identity management software (proGres versions 1 to 3) into the PRIMES ecosystem allows to address deficiencies as well as the further development in view of changing business needs. That means that blockchain distributed ledger (or other appropriate technology) as a technological building block and the applications in support of a Trust Scheme for Refugees that are being put forward in this RFP, namely a self-managed Digital Wallet for individual refugees and document verification registers (e-Registry and e-Apostille) are going to be part of an enlarged PRIMES ecosystem.

2. Project Methodology and Phases

The provider will be required to comply with UNHCR Project management methodology, broadly based on PRINCE2 (Projects IN Controlled Environments) a process based methodology for project management.

The information below is provided to serve as a high-level view of the Project stages, following the award of contract to the successful bidder:

Requirement Confirmation Phase

A UNHCR Project Team will finalize the business, IT and non-functional requirements for the new PRIMES extensions covered by this RFP, namely digital wallet and applications generating e-Registry entries (CRoA) and e-Apostilles, after proposals have been received and evaluated. This sequence is necessary in order to ensure that all risks and opportunities of the new technology are being taken into account. Fraunhofer Gesellschaft will advise UNHCR during this process.

Finalization of Detailed Specifications

The successful bidder will be invited to participate in the finalization of the ToR, as well as an opportunity to meet with key UNHCR personnel in order to establish a clear understanding of detailed requirements. External parties, such as refugees, public notaries, institutions of higher education and national regulators will also be consulted.

Design and Development Phase

UNHCR will align with the selected contractor methodology for the development processes, preferably an agile development methodology. This phase will include a Proof of Concept.

Testing and Pilot Phase

As the development of the application will be done by the contractor, the responsibility for code review, unit tests and integration tests will rest with the contractor and will be executed in their premises.

Once the development and the internal testing are completed at the contractor level, the application will be delivered to UNHCR for User Acceptance Test (UAT). The UAT will take place in those operations selected for the DAFI pilot projects, most likely in Jordan, Kenya, and Mauretania and will be performed by different stakeholders (= users, see definition under "3. Functional Requirements").

The UAT phase will be subdivided into: Regression, Architecture, Performance test, and Business Acceptance testing.

Documentation Phase

The documentation phase encompasses the drafting of all documents necessary for current use and to support the application after release. The documents will at least include: technical documentation, a user manual, an administrator manual, documentation of the schema, if there is a database in the backend, Help Files, FAQs (Frequently asked questions).

Receipt of Product

To confirm the receipt of the product the final delivery of the actual product and the handover of source codes is expected. The handover of all above mentioned documentation including user manual, administration manual, database schema, help files and other technical documentation is also necessary to confirm the final receipt of the product.

3. Functional Requirements

The applications to be developed serve the following high level and intertwined objectives:

Each refugee should be able to request access and have agency over his/her data held by UNHCR. S/he should be able to manage these data elements and add new data elements through digitalization, updating and uploading. For the data in the refugees' digital wallet to be useful and practical, the data has to be verified and certified within a Trust Scheme set-up by UNHCR.

Hence, a user according to these ToR can – depending on the context - either be a refugee, a UNHCR employee, or a person or institution that has been accredited by UNHCR to be a partner in its Trust Scheme.

3.1. Accessing and Managing Data and Documents into a Digital Wallet

UNHCR holds data on approximately 8 million individual asylum-seekers, refugees, stateless or other forcibly displaced persons. The organization has issued different types of identity tokens, either on paper or plastic cards, to an equally high number of persons.

Given that the various components of PRIMES have been designed to be auditable, meta data on all actions taken and documents issued, are part of the system. A refugee under the pilot scheme that is subject of this RFP may request data generated and held by UNHCR to be made accessible, editable and manageable in the wallet. Hence, UNHCR needs to come up with pre-defined data sets that can be transferred. The data set can be a single data field (date of birth for example) or numerous data fields as it happens when UNHCR issues attestations and ID cards. Pictures and biometric data also fall under this category of data set. In addition to transferring a data set, the system should generate automatically two further actions:

- A Certified Record of Action (CRoA) will be sent and stored in an distributed ledger (e-Registry)
- An e-Apostille providing meta data and confirming that the data is genuine should be attached to the transferred data set.

3.2. Future Data and Documents

Once a refugee has taken control of his Digital Wallet, he might want to add other documents that are either not yet generated by UNHCR or have been issued by a third party. Given that the target population for this pilot project are refugees that apply or receive DAFI scholarships, experience that these individuals normally submit the following documents:

- A birth certificate and/or an ID document
- UNHCR or Host Government issued document proofing their legal status as "refugee"
- UNHCR generated attestations on their family composition and economic situation
- Academic credentials issued by third parties.

UNHCR or another authorized entity in the UNHCR Trust Scheme would verify the document, digitize it and upload it into the Digital Wallet. In addition to uploading such data sets, the system should generate automatically two further actions:

- A Certified Record of Action (CRoA) will be sent and stored in a distributed ledger (e-Registry)
- An e-Apostille providing meta data and confirming that the data is genuine should be attached to the transferred data set.

3.3. Trust Policy and Standard Operating Procedures

As a pre-requisite for the successful completion of the project, a provisional version of a UNHCR Trust Policy will be required. That document will be ready by 15 December 2018. On the basis of the policy, the project should develop generic Standard Operating Procedures (SOP) taking into account the technical solutions developed.

3.4. Interoperability, Supplier and Device Neutrality

As UNHCR works with various partners, including NGOs and government entities, a resilient, and state-of-the-art electronic data interchange scheme will further leverage exchange with partners. The Trust Scheme will expand collaboration to include new entities and partners, in particular in the private sector. It is therefore imperative creating a platform that is interoperable and responsive to the needs of various users.

Interoperability increases efficiency and allows multiple stakeholders to leverage the benefits of the identification and trust system, both within a country and across borders. This includes the ability of different databases or registries (e.g., national ID and civil registration systems) to communicate with each other and/or exchange information in a timely and low-cost manner, subject to appropriate privacy and security safeguards.

UNHCR is committed to promoting open standards and ensuring supplier, device and technology neutrality. Open standards and design principles enable market-based competition and innovation. They are essential for greater efficiency and improved functionality. In particular for refugees, but likewise for all users, supplier, device, and technology neutrality is a must. No user should find himself in a supplier "lock-in," which are likely to increase costs and reduce flexibility to accommodate changes over time. Technology neutrality and diversity should be fostered to increase flexibility and avoid system design that is not fit for purpose or suitable to meet policy and development objectives.

3.5. Offline Capabilities

It is critical for users, especially holders of Digital Wallets, to access the data offline prior to online synchronization, on a mobile phone for example. No or low bandwidth services, often provided in remote locations with little or no connectivity make this inevitable. Subsequently, offline/online capabilities will be one of the main components of the solution.

3.6. Registration Principles

UNHCR offices register asylum seekers, refugees, stateless and other forcibly displaced persons, or persons whose status will be determined over time. An individual is always individually registered and assigned a unique ID that does not change over the life cycle as a person of concern to UNHCR. Individuals are registered within a Group. The nature of the group and the rationale for a particular group is mainly defined by blood relation and social bonds that can be locally specific depending on the location and the population concerned. Individuals may have different roles within a group. An individual can move from one group to another, e.g. an individual who was upon registration initially a member of the group of his/her parents, got married and became now a member of a group with the spouse.

There are two ways of registering individuals

- Registration focusing on the detailed individual data which is called Individual Registration
- Registration focusing on the group level data and where individual information is minimal which is called Group Level Registration

Many documents will display the group ID and the group ID is more often used for working with persons of concern than the individual ID as UNHCR often works with families and seeks to maintain family unity as a principle. *However, for the purposes of this pilot project, only processes relating to individuals will be developed and individually assigned Digital Wallets created. However, the technical solution presented should allow to understand with which group(s) and individual is associated and should allow the development of group-centred processes at a later stage.*

3.7. Individual Registration Data

PRIMES allows for a continuous registration process by

- Adding and continuously updating information regarding individuals in the database
- Registering in a group context (each individual must belong to a group)
- Applying a unique individual ID (Each individual has a unique individual ID)
- Allowing global mandatory fields
- Allowing local mandatory fields as well as optional fields
- Applying validation rules which can be globally or locally configured
- Allowing partners to execute registration (incl. for persons who are not of concern to UNHCR)
- Verifying registration done by partners
- Transforming group level registration data into full blown individual registration data.

Individuals can be registered either by UNHCR, a government or another partner. If a person is registered by a partner, the record might need to go through a validation step in order to be fully registered with UNHCR. The individual registration is the information back-bone. The individual records will go through UNHCR/Partner processes managed throughout a wide range of functionalities.

The individual registration data mainly includes the following information and records:

- Bio-data – One record per individual and name change history; (many data elements ranging from name to nationality fall under bio-data or foundational data.)
- Family Relationships
- Legal Status
- Addresses – Multiple addresses, various address types
- Displacement History / Onward Multiple Movements
- GPS location
- Phone/e-mail – Set-up for bulk messaging
- Alias – Tracking of other identities
- Education – Recording of education history
- Occupation/skills – Recording of occupation and skills history
- Relatives – Individuals who are not registered in proGres
- Languages – Recording of language skills
- Documents – Recording of documents (provided by or to an individual)
- Photos – Photo history, direct capture or import.
- Property – Recording of main property e.g. House in Country of Origin
- Specific Needs – Multiple specific needs. Semi-automated based on rules.
- Role – Specifying e.g. food collector.
- Individual Notes – Recording of notes related to an individual
- Legal Status – e.g. Refugee, Asylum-Seeker
- Links to other groups/individuals

The system is able to record and update detailed information related to individuals. This includes registration of new arrivals, departures, births and deaths, inactivation as well as reactivation.

3.8. Status Determination

Refugee Status Determination (RSD) is a complex process based on elaborate workflows which are recorded and processed through proGres v4 case management module. RSD starts with the identification of individuals and involves registration, interviews, referrals, assessments, decisions, notifications and counselling. However, for the purposes of this pilot project, only data that relate to the outcome of the process (negative or positive), i.e. the assigned status, are relevant. In practice this would mean that notifications on status issues are part of the new system.

Status notifications may include:

- Derivative status

One may be recognized as a refugee in the capacity of a close family member of a recognized refugee based on the right to family unity.

- Exclusion

Exclusion is the stage of the process where it is assessed that an individual who meets the refugee criteria is nevertheless denied international refugee protection because he or she receives protection or assistance from a UN agency other than UNHCR or is not in need, or not deserving, of such protection.

- Cessation

Once a refugee is able to safely return and re-establish him or herself in the country of origin or habitual residence, or obtains the full protection as a citizen of another country, international protection is no longer justified or necessary. If this is the case, the asylum country or UNHCR may decide that his or her refugee status shall come to an end.

- Revocation

Revocation of refugee status is the withdrawal of refugee status from a person properly recognized as a refugee, who engages in conduct within the scope of acts that makes him or her undeserving of international protection after recognition.

- Cancellation

In a situation where reliable information calls into question the correctness of a refugee status recognition which has become final, it will be appropriate to examine whether there is sufficient basis for initiating procedures with a view to the possible cancellation of refugee status – that is, invalidating it with effect from the time of the initial decision.

Complementary and temporary protection:
A person in need of international protection found not to meet the criteria set in the above-mentioned legal instruments may be granted complementary forms of protection. Some States have also provided "temporary protection" in situations where large numbers of people had fled situations of generalized violence and/or armed conflict as a pragmatic short term measure without however making a determination on their status.

3.9. Statelessness

In addition to its mandate to protect refugees, UNHCR also has a global mandate to protect stateless persons. As in refugee status determination, UNHCR can assess, whether to the Office's knowledge, a person is stateless or possesses a specific nationality. Assessments of whether a person is stateless may be necessary in order to subsequently assist the individual to document links to a State and acquire protection from that State, or, potentially, confirm, acquire or re-acquire nationality. Nationality is just one – albeit important – attribute of a person's identity. Being stateless therefore does not mean that the person should not benefit from the trust services offered by UNHCR.

3.10. Assistance

UNHCR offices provide assistance covering a wide range of types such as food, non-food items (NFI), cash assistance (including simple loans), education, counselling, psychosocial and medical assistance. Assistance can relate to individuals or groups. The pilot project relates to tertiary education only but should allow for expansion into other fields of assistance and their management at a later stage. Notifications on eligibility for assistance or that a scholarship was granted should be part of the new system.

3.11. Resettlement

Resettlement in a third country is one of the three possible durable solution options for refugees. Like in RSD, the process is complex. However, for the purposes of this pilot project, only data that relate to the general current state in the resettlement process and the outcome of the process (pending, negative or positive), are relevant. In practice this would mean that notifications on status and outcome should be part of the new system.

3.12. Voluntary Repatriation

The process of voluntary repatriation, another one of the three durable solutions, is the return of refugees from country of asylum to country of origin. UNHCR promotes and advocates the fact that the return process should be voluntary, safe and executed with dignity. The PRIMES based VolRep procedures are not relevant for the planned pilot project. An individual who is undergoing or underwent VolRep is not eligible for a DAFI scholarship.

3.13. Protection Case Management

While protection case management is not relevant for the pilot, a current status or an assessed protection need might impact the socio economic vulnerability, which constitutes a DAFI selection criteria. The new system should therefore allow to take a notification on status or outcome into account.

4. Other Business Processes

4.1. Access Rights Management and Data Sharing

This section encompasses the following needs:

Controlling access within the Trust Scheme

- Allowing for distinct access by different users
- Allowing for record -, field- and value based access.
- Defining user access to menu lists
- Defining user access to views (functional, geographical or other), tables or documents

- Sharing and transferring information
- For referral, information or further action

Controlling Access within proGres

A user's access to proGres will be limited to the functions he performs or the information he needs.

That remains the same for UNHCR staff. To that purpose, the following is to be covered:

- Each proGres user is assigned to one or many functional roles.
- It is possible to change a user's functional role(s)
- Each user's role(s) define(s) the appropriate level of <Read, Update, Create, Delete> applied to his access rights on views (functional, geographical or other), tables, fields and field values and documents.
- Similar, but different rights are applied to users at menu list and field level.
- Sharing Data within proGres
- It is possible to share data with an authorized user for information, referral or further action.
- Defined user actions or automatically triggered workflow events open rights to allow for information sharing.

The protection of highly sensitive information makes access rights management and data sharing a core part of the information system. As a consequence, the proposed design must be intuitive, easy to use and fit to purpose and easy to administer.

4.2. Reporting and Digital Document Production

As any other business, UNHCR has important reporting needs. The reporting features should support analysis and business decision-making by providing historical, current, trends and predictive views of business operations. It should include all typical management reporting capability, such as:

- Statistical reporting
- Controlling Listing
- Benchmarking
- Performance
- Trend tracking
- Etc.

In addition, specific ad-hoc reports might be created in the future to cater to specific situations or processes. Due to the large number and variance of reporting needs and the fact that most of them would be specific to an operation or an individual office, UNHCR will require a solution that will allow users to create, manipulate and change their own reports, thus reducing reliance of the user community on IT specialists for report-creating purposes.

As what regards reporting addition and publication, the system shall provide all the necessary mechanisms to distribute and share reports within the Trust Scheme user community. The following features should also be provided:

- Access to reports will depend on user access rights

- Reports will be available on-demand from a dedicated screen in the application or from a dashboard that would be configurable by the user
- Users will be able to define how they want to view and distribute their reports [e.g. Dashboard, Printouts (Word, PDF, Excel, XML…), and email listing …]
- Scheduling and automatic batch reports with defined distribution rules

Please note that UNHCR uses different BI solutions.

In addition to reports, the application must support the production of digital documents as well as Certified Records of Action (CRoA) for the planned e-Registry and e-Apostilles to be attached to digital documents.

4.3. Shared Features in Reporting and Document Production

Several requirements are shared between reporting and document production. These include:

- The management of reports and document templates (create, edit, delete), their execution (visibility in the UI, availability to the users) are subject to specific access rights. Not all users will have the rights to handle reports and document templates.
- Need to support Multilanguage, including right-to-left support for Arabic.
- Both of the above features will be used by non-IT staff, so they should be easy and intuitive and provide step-by-step on-screen guidance for design and generation of reports and documents
- Distribution of reports/documents should be easily managed as they can be deployed throughout the whole organization, a region, a country, an office or just a subset of users.
- A history of document production and issuance should be maintained so that users know exactly which documents have been issued, cancelled, replaced, recalled, or destroyed.
- Different users should be able to generate documents and run reports according to their user access rights.
- Documents includes certificates, ID cards, entitlement documents, attestations, certificates and more.
- Information and content can be distributed through different reports (e.g. dashboards, printouts (Word, Excel, XML) etc.]

4.4. Record Management, Changing UI Language and Contextual Help

In proGres record management in this perspective covers advanced search, the ability to save search profiles, the ability to save search criteria, creating and managing filters.

The requested features are as follows:

- Federated search: i.e. search through documents of different types (Word, PDF, Excel…)
- Searching on document metadata, in addition to the common search on document content
- Advanced multi-criterion search as a common feature. That will reduce the number of reports required as a result of insufficient searching capabilities
- Search within a search result
- Display search results either as a list of records or as aggregated statistics.
- Saving search profiles and managing shortcuts as standard in the industry today

4.5. Multi-Language User Interface

System must support multi-language user interface. The user should be able to choose an option from a pre-defined list of languages to view screens, menus, field names, reports and Help pages in their preferred language.

The required languages are English, French, Spanish and Arabic (left to right). Default language shall be English. Users must be able to specify and save their language preferences so next time they login, the system will automatically display the language of their choice without a need to go through a language change process again.

The system must be able to accommodate new language requirements in the future and offer a simple way to add a new language without an extensive development effort.

4.6. Contextual Help

User help must support the multi-language user interface requirement. User should be able to browse via Help topics and search by keywords in their choice of pre-defined languages. Help pages should be available at all levels (e.g. Menu, screen, field) providing context and relevant tips to users.

4.7. Self-Service Module / Digital Wallet

Self-service is an optional functionality available through the Web to persons, already registered in proGres. Thereby a Digital Wallet is being created that could be accessed on multiple devices.

It allows the following options:

- Viewing relevant personal data (which may be related to workflows)
- Printing relevant data (which may be related to workflows)
- Sending messages to UNHCR staff through a selected category (e.g. Education Officers etc.)
- Requesting for Interview with UNHCR; Re-schedule an Interview

Access to the self-service function will be subject to security regulations and at the request of the individual only. For the purposes of this pilot project, access to the Digital Wallet will be restricted to refugees applying for or receiving DAFI scholarships only.

User Interface of the Digital Wallet must support multi-language requirements and should be available initially in English, French and Arabic. In the long run, the system must allow extension and addition of other languages.

The Digital Wallet must be configurable (locally and at the central level), for example:

- The Self-service function can be switched on and off
- Features available via self-service can be enabled or disabled - for example, combinations of the three options (Viewing, Printing, Sending)

4.8. Referral

Referrals consist in passing over documents or tasks to another party for further action or information (e.g. approval, review update). Referrals are an essential element of every functional workflow in *proGres*.

It shall be possible to send free text messages in referrals.

Referrals shall be hyperlinked to relevant individuals/processing group or to functionalities

Referrals are requests to get involvement and can be sent to:

- A single user
- Functional unit users (fixed group of users) e.g. Field Office protection unit users
- Ad-hoc created group of users e.g. HUB resettlement reviewers

Referrals can be system generated

- Workflow triggered (e.g. inactivating user will automatically refer all cases pending with that user to the supervisor)
- Information triggered (e.g. recording unaccompanied minor specific need would result in automatic referral to Community Service staff)

Referrals can be user generated

- One way referrals:
- Originator does not expect any feedback from recipient
- Case referred for scheduling for interview with third party
- Two way referrals – recipient is expected to provide feedback to originator

Referrals are linked to or complementing:

- Alerts and notifications
- Work list
- E-mail
- Referrals can be retracted, rejected, or delegated, with notification.

4.9. Alerts/Notifications

Alerts and notifications are an essential element of every functional workflow. It must be somewhat self-explanatory as to the time and event factors driving them.

For this TOR, it is understood that alerts are time-driven, whereas notifications are event-driven.

They have the following characteristics and functionalities:

System or a user communicates with:

- Single user
- Functional unit group of users e..g. field office protection unit users

- All branch office users
- All active users, etc.
- Ad-hoc created groups of users e.g. branch office RSD reviewers, Resettlement schedulers, Registration unit front office users,

Linked to or complementing

- Work lists:
- Automatic reminders on pending actions
- E-mail
- user generated email
- Ad hoc reminders on outstanding referrals
- System generated reminders on e.g. referrals
- Various system messages
- General system alerts: e.g. prompting user to change login password
- Erroneous entries: e.g. value recorded cannot be validated
- Ambiguous entries e.g. combination of values recorded in different fields unlikely
- Incomplete entries e.g. Mandatory fields empty
- Other system alerts e.g. server timed out, login timed out, etc.
- Sensitive actions taken, therefore, requiring confirmation e.g. Inactivating groups or individuals, _ changing bio data or photographs, submitting cases for resettlement consideration, etc.
- Workflow triggered e.g. urgent referral received, internal message received, etc.
- Recording specific information triggered
- Automatic reminders e.g. approaching set deadlines

4.10. Form Builder

proGres allows the operations to create their own forms which can be used to capture various types of information linked to the individual or group records. The form enables the operations to record data which is not part of the standard database fields. Typically it could be assessment forms, questionnaires, surveys on ad hoc basis.

The main functionalities include:

- Specific user types can create and design Electronic Form Templates (Soft-forms)
- Specific User types can copy and modify existing templates for new templates
- Specific users can inactivate or delete forms (deleting will also delete data)
- Form templates can be shared among users and user groups

The user can determine in the electronic form template design, whether a form can be executed only once or multiple times for the same individual/group. Some forms might be used e.g. on a periodic basis and the user will therefore need to keep a history of the forms for an individual/group.

Forms can be related to individual records, group records or workflows.

Electronic forms can include

- pre-defined data types
- defined code values
- validation rules

- skip-logic
- error messages
- upload document function
- the forms can have pages and sub-forms

Users can perform data analysis, data export and reporting functions
Possibility to print blank or filled in forms
Possibility to identify a survey population for which a given form will be available
The electronic forms can be linked to workflows.

4.11. Document Management

This is relates to the management of all type of documents and images that are to be associated with an individual or a group record within PRIMES primarily *proGres*

This includes the documents generated from *proGres* and documents from external sources:

- Scanned documents
- Files received from partners

The requirement is to have a comprehensive and integrated document management system with storage, version control, advanced searching capabilities and the possibility to have links between documents. The features include federated search and the use of content metadata. User access rights should be managed.

Document generation is specified in "Reporting"

All executed print jobs shall be logged.

4.12. Document Upload

The process of document upload is a functionality that allows users to attach an electronic file to a group or individual record.

The user requires the functionality to:

- Add/remove a document link to a record
- Keep documents link accessible even when the record moves to a different location within or outside of the country
- Link any type of document (word, excel, pdf, jpg etc.)

4.13. Batch Operations

ProGres allows for batch updates.

Batch updates can be performed for:

- Records identified using a search criteria - however some core set of data cannot be batch updated

- Records within a workflow
- Records with a functional view
- Records when working in offline mode
- Printing multiple documents and many same documents at once

Batch updates have the following characteristics:

- The user is able to roll-back a batch operation
- The user is able to cross-reference data from an external list and batch update records that are matching or non-matching.
- The user should be able to produce a report after that.
- The user is able to cross-reference data from an external list and update matching records with the data in that list.
- The user should be able to produce a report after that.

Permission to perform batch operation is defined through the security profile. This functionality shall also be available for partners.

4.14. Configuration and Customization

This section describes the *proGres* application's ability for configuration and customization around main areas of concern. Configuration and customization are possible down to the lowest geographical or functional working unit.

The main areas of concern reflected throughout this TOR are the following:

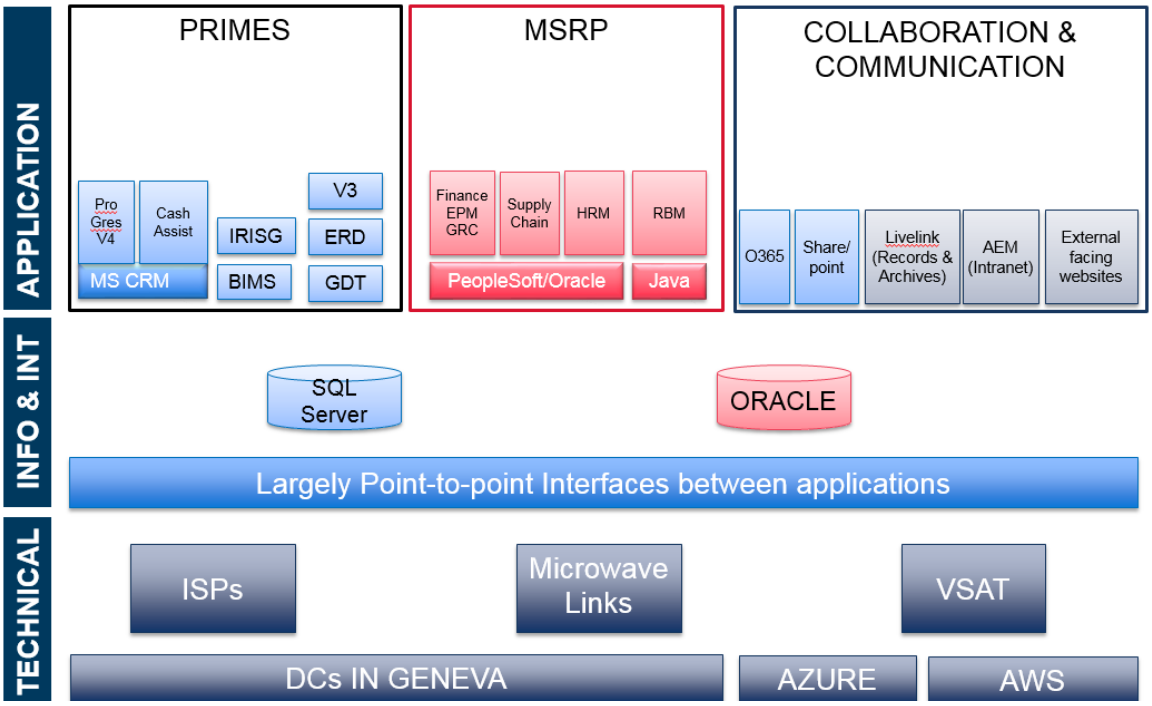
- Connectivity
  - Online operation
  - Offline operation
- Data sharing
  - Interface with partners – how the information is shared with different offline partners using other data processing systems
- User interface
  - Language
  - Labels
  - Menus and toolbars - Fields
  - Column or row sizes
- Dataset
  - Available fields
  - Mandatory fields
- Workflow
  - Global templates
  - Mandatory elements at global, regional and local level
  - Optional elements
- Codes and descriptions
  - Address elements
  - Detention facilities
  - Resettlement quotas
  - Other locally specific codes and descriptions
- User rights
  - Access to elements of dataset
  - Access to functionalities (menus)

- User groups
  - Functional units' groups
  - Ad-hoc created groups
  - Partner groups
- Work lists
  - Displaying elements of individual workflows
- Alerts and notifications
- Reporting
  - Statistical reporting
  - Performance reporting

5. Technical Architecture

Bidders must provide a solution which can evolve with UNHCR's infrastructure trends and cater with the current environment.

5.1. High Level Overview of IT Architecture in UNHCR



5.2. Client Computer

	Current	Future

Operating System	Windows 7	Windows 10
Office application	Ms Office 2010	
Web Browser	Internet Explorer 10 FireFox 31.0	Internet Explorer 16
E-mail system	Outlook 365	
Anti-virus	McAfee	In process of being determined

Database: There are two standard database servers in UNHCR:

Microsoft SQL Server 2012
Oracle 12g

Microsoft SQL Server is used by ***proGres*** and all Persons of Concern databases and Oracle by all back-office applications e.g. MSRP and Focus.

Operating Systems:

	Current	**Future**
Microsoft environment	Windows 2012	
Oracle environment	Oracle Enterprise Linux R5	
Unix Application	Linux Ubuntu	

5.3. Network

Connectivity is not available in all locations where UNHCR offices operate and where refugee registration must take place.
Average bandwidth is low in UNHCR field operations.
System needs to be available even if the connectivity to the central repository is down.

5.4. Application Infrastructure

This chapter captures the basic requirements to be incorporated in the application infrastructure.

proGres' architecture is based on a modular principle. An individual module component is a software package (i.e. a web service or module) that encapsulates a set of related functions (or data).

proGres is built on CRM dynamics.

Its architecture improves maintainability by enforcing logical boundaries between components.

proGres provides the functionality to configure and exchange data with other IT systems and System Log services.

5.5. User Interface

A web interface or a mobile interface shall be provided by the application to the user. The interface shall be compatible with all major web browsers.

Plug-ins & API

proGres will not support all business or technical needs, as some of them could be exceptions.

However, this does not mean that the needs are ignored. To answer the need of external systems integrating with proGres), the application provides for a plug-in mechanism by use of API.

ProGres provides services which the plug-ins can use, including a way for plug-ins to register themselves with the host application and a protocol for the exchange of data with plug-ins. Plug-ins depend on the services provided by the application and do not usually work by themselves.

Conversely, ***proGres*** operates independently from the plug-ins, making it possible for authorized users to add and update plug-ins dynamically without having to make changes to the system.

The ***proGres*** Application programming interface (API) does provide standard interfaces allowing third parties to create plug-ins that will interact with the application/databases. The API architecture shall be:

- Secure and reliable.
- Easy to learn.
- Hard to misuse.
- Rather easy to extend.

The API design decisions were made to minimize the impact on performance and security.

5.6. Database Architecture

5.6.1. Database architecture overview

The ***proGres*** application uses a centralised database architecture.

This database(s) stores the entire refugee data collected by UNHCR and its partners.

The choice of having a centralised database was driven by the following needs:

- Ensure reliability of data in all UNHCR and partner operations by accessing the same set of data at any point of time
- Ease of data sharing and referring across UNHCR staff/offices and partners
- Improved data security
- Centralised IT administration, allowing to reduce cost of maintenance, upgrades and enhancements and improve data security
- Alignment with the overall UNHCR organisational structure

5.6.2. Centralised database concept

UNHCR's centralised database respects the following principles:

- Ensuring system availability (24/7/365[2]); system down time is not acceptable due to the nature of UNHCR's work with persons of concern.
- Manageability - the system shall be easy to maintain. It includes such general IT maintenance tasks as backup and restore procedure, simplified release and update management etc.
- Distribution of data shall be transparent to the users
- Users shall interact with the system(s) and its components as if it is one logical system; this applies to system performance, method of access etc.
- Transparent transactions: each transaction must maintain the data integrity (see below).
- Cost effectiveness of IT maintenance and support via a regional/central Help Desk

5.6.3. Database Replication and Kiosk Mode

- proGres has database replication and failover, which allows the system to run uninterrupted in case of failure of the main DB

5.7. Transactions Management

All transactions follow A.C.I.D. property:

- Atomicity: the transaction takes place as whole or not at all. An atomic transaction cannot be subdivided and must be processed in its entirety or not at all. Atomicity means that users do not have to worry about the effect of incomplete transactions.
- Consistency, maps one consistent database state to another;
- Isolation, each transaction sees a consistent DB. Isolation refers to the requirement that other operations cannot access data that has been modified during a transaction that has not yet completed. The question of isolation occurs in case of concurrent transactions (multiple transactions occurring at the same time)
- Durability, the results of a transaction must survive system failures

5.8. Backup requirement

As proGres was deployed in multiple geographic locations around the world, the system was designed in such a way that it supports dynamic backup.

Even if this principle involves certain risks (e.g. if the data is altered while the backup is in progress, the resulting copy may not match the final state of the data), a resolution mechanism to avoid data inconsistency when recovery is necessary is available.

It was designed to allow recovery of certain parts of the database without impacting the whole data contained within the system. For instance, in the case of a data corruption in a particular office, the database administrator should be able to recover the data of that office only, without affecting any other UNCHR/partners offices.

Furthermore, the recovery period should be as short as possible.

Finally, due to its sensitivity of the data, the backup must be encrypted.

5.9. User Devices

The system needs to allow for different types of user devices. It needs to allow for Android and IOS.

It needs to be accessible from a computer.

It needs to be adoptable to any new technique.

It needs to be GSM enabled.

It needs to allow for any up to date user device.

Annex 4

Glossary of Terms

Cognos: Product used by UNHCR as a Business Intelligence and financial performance management

Digital Identity: A digital identity is information on an entity used by computer systems to represent an external agent. That agent may be a person, organization, application, or device. ISO/IEC 24760-1 defines identity as "set of attributes related to an entity". Digital identities allow access to computers and the services they provide to be automated. Digital identities make it possible for computers to mediate relationships. The term has also come to denote aspects of legal and personal identity that have resulted from the widespread use of identity information to represent people in computer systems.

Digital Inclusion: Many refugees spend much of their life without access to the everyday digital services that many take for granted. This situation might be compounded by the lack of personal ID documents. This halts their ability to connect with the world and leaves them excluded - unable to participate, develop and build self-reliance. Access to digital based services is a necessity so as to obtain documents (case management), cash assistance, accelerating learning, training, banking and other commercial transactions, as well as employment. UNHCR advocates for new forms of identity affirmation (even in the absence of legal ID documents) that will allow for universal or partial access to information, official records, services, and commercial models and transactions. A major challenge in this context is illiteracy and the digital divide, i.e. the fact that many refugees live in an (almost) off-line environment. How can we overcome these constraints and use advances in AI, voice driven services, automated translation, and the use of icons to be put at the service of refugees. Digital inclusion should provide access to online educational and training as well as economic and employment opportunities and mitigate the risks for an already vulnerable population to avoid exploitation and further (digital) marginalization.

Digital Wallet: Is a system that securely stores user generated information, documents and passwords. While it maybe used for numerous payment methods and websites, UNHCR's approach considering the population it serves, is rather that of a file repository. In setting-up such systems, UNHCR will follow international technology regulation, standards and interoperability.

Economic Identity: In a presentation by WFP, economic identity was defined as verified information on a person that allows to open bank accounts and/or prove some type of credit history or payment behaviour. An economic identity facilitates economic participation. It can be based on (or does not necessarily lack the connection) to legal identity. Economic identity should be an automated by-product of a well-established digital identity.

Identity: In general usage, identity may be defined as "the characteristics determining who or what a person or thing is" (OED). For UNHCR's purposes, however, this definition requires two further qualifications, namely it must possess the quality of continuity over time and attain and retain the quality of uniqueness. Accordingly, the term identity is defined as a combination of characteristics (biographical, physical, legal, social, economic) which uniquely and enduringly differentiates a given individual from all others. It is recognized that certain elements of an individual's identity are dynamic and may change over time or be presented differently depending on circumstances and required purpose.

Identity Management: UNHCR's working definition of identity management is the recording, strengthening, preserving and utilizing of identity records, for the purposes of empowering persons of concern, promoting access to rights, promoting programmatic efficiency and integrity, and facilitating protection and durable solutions. Identity management is in effect a framework that provides consistency and cohesion to its various component parts. Registration, including the associated processes and tools,

is one of the components of identity management. In the IT industry ID management is often used synonymously with identity rights management, i.e. organizing the access, use, distribution, and management of data across administrative domains as well as within Web services environments. It is, in effect, a way to protect sensitive information while simultaneously allowing fluid collaboration. UNHCR is still exploring ID self-management as a measure of empowerment in and complementarity to its own ID management activities.

IDP: Internally-displaced person or persons, i.e. a forcibly displaced persons living in his/her own country.

Know Your Customer/Client (KYC): A standard procedure in the financial industry in order to obtain detailed information about a client's risk tolerance and financial position and to assess and monitor customer risk and a legal requirement to comply with Anti-Money Laundering (AML) Laws. It is a fundamental practice to protect financial institutions from fraud and losses due to illegal funds and transactions. KYC refers to the following steps taken by a financial institution (or business) to:

- Establish customer identity
- Understand the nature of the customer's activities (primary goal is to satisfy that the source of the customer's funds is legitimate)
- Assess money laundering risks associated with that customer for purposes of monitoring the customer's activities

Lack of alternative technological solutions: This is a criterion for evaluation of submissions by UNHCR. It considers whether or not other technologies or tools are already applied or have been proposed for this use case. While there may not always be a direct one to one alternative to the proposed technology solution, it may be the case that there are alternatives for similar use cases.

Legal Identity: The term refers to the legal personality of natural persons capable of holding legal rights and obligations within a country and/or a legal system, such as entering into contracts, suing, and being sued. Legal personality is a prerequisite to legal capacity, the ability of any legal person to amend (enter into, transfer, etc.) rights and obligations. Human beings acquire legal personhood upon registration/recognition by the competent authorities of a State, ordinarily occurring at birth or soon afterwards. Documentation issued by the State, including birth certificates, provides evidence of a person's legal identity.

LIGHTest: This abbreviation stands for "Lightweight Infrastructure for Global Heterogeneous Trust management in support of an open Ecosystem of Stakeholders and Trust schemes" www.lightest.eu// The objective of the LIGHTest project is the creation of a global cross-domain trust infrastructure that renders it transparent and easy for verifiers to evaluate electronic transactions.

Levels of Assurance (LoA): This concept describes the degree of certainty within a trust scheme that a user has been properly identified and presented a credential for authentication that refers to his or her identity. In this context, assurance is defined as (1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and (2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. In the European eIDAS system the following assurance levels (score) are being assigned for electronic identification: low, substantial, and high.

Node: A participant in the blockchain network that stores an exact copy of the ledger. Each time a transaction is carried out and approved, all the nodes update the ledger thus maintaining a distributed and synchronized copy.

Permissioned Blockchain: One way to classify blockchains can be according to the permissions to read and write in the ledger. A permission-less blockchain is a network in which any participant can openly read

and write while a permissioned blockchain limits the number of participants with such rights. The definition often overlaps with "private Blockchain".

PRIMES: Abbreviation for UNHCR's "Population Registration and Identity Management EcoSystem". A system of applications for population management built around a population registry that is part of version 4 of ProGres (Profile Global Registration System).

Privacy challenges: In the context of this RfP this refers to the protection of personal data and sensitive information. It is especially important to know what and how sensitive information is stored and identity information, documents, certificates etc. are protected and kept confidential.

Private Blockchain: A Blockchain operated and controlled by a single organization or a defined consortium of organizations (also: consortium blockchain). The access to read and write is fully controlled by this organization but can be extended outside of it. The definition often overlaps with "permissioned blockchain".

Public Blockchain: A Blockchain where anyone can view what is on the Blockchain and participate, without permission. Anyone can send transactions to the blockchain and participate in the consensus process – the process that determines which information gets added to the blockchain and what its current state is.

RSD: Refugee status determination

Scalability (to whole organization): Blockchain public ledger applications are limited in terms of transaction speed and due to the size of the nodes that each need to store all information that is stored on the blockchain. Use cases that are very dependent on transaction speed or need to store a significant amount of data, might work in a small-scale pilot, but would face challenges if applied to the organization as a whole. Scalability is of course similarly important if another technology and not blockchain is applied.

Technical feasibility: This contemplates on if the proposed solution could be applied in a pilot and have access to all of the necessary information and resources needed to implement a pilot. Further, it considers if the use case is feasible with a blockchain distributed ledger (or other proposed technology) infrastructure component.

Transactional Identity: A transactional identity refers to enable action, i.e. an identity which allows a person to do something. This is not the same as a transaction ID, which is an automatically generated and serialized hash in a network.

Trust Scheme / Trust Authority: A Trust Scheme is operated by a Trust Scheme Authority and comprises the organizational, regulatory/legal, and technical measures to assert trust-relevant attributes about enrolled Entities in a given domain of trust. See annex 2 above.

Use of specific blockchain features: This criteria for evaluation of proposals examines if the features and main components of blockchain are applied in an advantageous and appropriate manner. The six main Blockchain concepts considered are; decentralization, immutability, security, consensus algorithms, smart contracts, and types of blockchain.

Annex 5

Tender Process and Evaluation of Offers

Timeline

Publication	Request for Proposals (RfP)	12 November 2018
Deadline	Questions	22 November 2018 (23:59 hrs CET)

(above deadline is for submission of questions that will be addressed at the Pitching Event)

Deadline	Registration for Pitching Event	22 November 2018
	Pitching Event in Copenhagen	27 November 2018
Deadline	Proposal handed in to UNHCR	18 January 2019 (23:59 hrs CET)
	Evaluation of proposals	1st Quarter 2019
Deadline	Contract awarded	before end March 2019
	Implementation of project	2019

General information

It is possible to hand in proposals as individual organizations or as consortia of organizations. Bidders willing to deliver their solutions in cooperation with other organizations can form a consortium. These consortia will have to sign a consortium agreement and agree on a leader of the consortium that will act as main point of contact for UNHCR. This leader should be clearly identified in the proposal. All partners will be jointly and severally responsible for performing the contract if it is awarded to them. Where a proposal is submitted by a consortium, the evaluation criteria relating to economic and financial capacity (see point 4 below) will be examined for each member. However, where a given threshold for economic and financial capacity and/or technical and professional capacity is required, the ability to meet it will be assessed in relation to the consortium as a whole.

Participation in the Pitching Event in Copenhagen is a non-mandatory condition to hand in a proposal and the pitches will not influence the formal evaluation. However, applicants are strongly encouraged to use the opportunity of this event to present their approach and engage in a dialogue with representatives of UNHCR before handing in their full proposals. To ensure that all applicants have access to the same information, the conference will be recorded and shared publicly. The recording will also include all questions put forward by participants at the Pitching event conference and the answers provided by UNHCR as well as any additional information shared publicly with all potential bidders. All interested bidders have an equal chance to participate in the Pitching event.

Evaluation of Offers

The procedures to be followed in preparing and submitting a proposal are defined in the covering letter for this RFP. The instructions and guidelines as well as the deadline for submission of proposals needs to be respected

The RFP process is governed by UNHCR's Financial and Procurement rules, which will be strictly adhered to throughout the RFP process. The RFP process is managed by the Procurement Service (PS) and any contact with UNHCR in relation to this RFP must be through the designated focal point within PS.

The detailed evaluation criteria are internal to UNHCR and will not be shared with any of the Bidders, neither prior to nor after the final submission date.

For the evaluation of the proposals a maximum of 100 points will be allocated. The evaluation methodology applies a 60 technical/40 financial ratio.

Technical Evaluation

The technical minimum passing score is set at 60. If a bid does not meet this minimum, it will be deemed technically non-compliant and will not proceed to the financial evaluation.

The Technical offer will be evaluated using the following criteria categories:

CRITERIA DESCRIPTION	**Score**
1. Quality of Service (work approach and methodology) (70%)	
Understanding of requirements	25
Novelty and Innovation	15
Incorporation into UNHCR environments and scalability beyond the pilot	15
Overall quality and clarity of proposal	15
2. Company Qualifications (20%)	
Relevant experience in software development	10
Relevant experience in the business or the number of ongoing similar and successfully completed projects	10
3. Personnel qualifications (10%)	
Relevant experience of core people who will work on the project	5
Technical support teams	5
TOTAL TECHNICAL SCORE	**100**

The technical offer should in total not exceed 30 pages and should be structured as follows:

1. Strategy: objectives, concept, approach and ambition of the project

2. Solution: technological and operational approach with a detailed description of proposal/solution addressing all criteria 1-3 mentioned above

3. Implementation: work plan, inputs/outputs (deliverables description)

4. Organization and management: quality, resources as well as risk management; organizational structure, roles/responsibilities, CVs, Letters of Intent of organizations involved in the proposal (can also be included in the Annex to the proposal)

Financial Evaluation

The financial offer will need to be submitted in a separate document (ideally in EXCEL as per below)

The bidder is expected to define the structure of the required HR resources (team) that will be suitable for delivering the specified product within the given time line. The bidder should choose its team and its team management and structure mindfully.

The team structure description needs to include the mandate of each key team member including a description of skills set and experience.

The financial offer shall include a detailed list of all cost elements in table format specifying the number of required HR resources, estimated days/HR resource as well as each HR resource's rate. Each cost element shall also be outlined with its total cost.

Some key cost elements which need to be outlined by the bidder are presented in the following non-exhaustive list:

Cost Element	Number of Human Resources (HR Type/ persons)	Estimated time (days)/ per HR type	Rate/per HR type/ per Day	Total
List of cost elements				
Review, understand and confirm detailed business requirements				
Complete the technical specifications				
Complete the application architecture				
Connection to PRIMES Ecosystem				
Development of the application as proof of concept				
Prepare and provide testing				
Deploy a proof of concept in a specified UNHCR location(s)				
Provide technical documentation and user guide				
Support pilot deployment, if relevant				
Warranty period where defects and bugs identified during pilot are fixed				
Additional proposed elements, add lines as required				
Consultancy Fees - Sub-total:				
Overhead, administration or other costs, if any (indicating nature and breakdown)				
Expected travel costs				
Management costs				
Add or remove lines as required				
Other costs - Sub-total:				
Total Project Costs (all inclusive)				
Additional cost elements related to scalability, if so (10.000 Users)				
Additional cost elements related to scalability, if so (100.000 Users)				
Additional cost elements related to scalability, if so (1 Mio Users)				
*The cost of the project will be calculated based on the total package price or the individual daily rates plus other expenses whichever is less.				

The Financial offer will use the following percentage distribution: 40% from the total score.

The maximum number of points will be allotted to the lowest price offer that is opened and compared among those invited firms. All other price offers will receive points in inverse proportion to the lowest price; e.g., [total Price Component] x [US$ lowest] \ [US$ other] = points for other supplier's Price Component. For evaluation purposes only, the offers submitted in currency other than US Dollars will be converted into US Dollars using the United Nations rate of exchange in effect on the date the submissions are due.

Proposals should be submitted electronically until 18 January 2019, (23:59 hrs CET) in PDF-format via E-Mail to **HQSMSBID@UNHCR.ORG**.