

Construction Industry One Registry System

Terms of Reference - Value Added Service Provider Eligibility

1. Introduction

The Construction Industry Authority of the Philippines, an agency attached to the Department of Trade and Industry, was created by virtue of Presidential Decree No. 1746 as a central agency that will promote the growth and development and address issues and challenges of the construction industry in coordination with other government agencies.

The Construction Manpower Development Foundation (CMDF), one of the implementing boards of CIAP, is mandated to “recommend appropriate policies and measures to rationalize training and export of trained manpower in the construction industry,” among others, in coordination with DOLE, DepEd, TESDA, and the Philippine Overseas Construction Board of the Construction Industry Authority of the Philippines (POCB-CIAP).

The CMDF is embarking on creating the Construction Industry One Registry System (CIORS) that will provide the following information and services to all relevant stakeholders:

A. Industry Snapshot

The CIORS will generate real time reports on indicators relevant to government policy makers. The system will provide information on the industry overview covering:

- workforce demographics
- number of jobs
- top employers
- unemployment rate of those previously employed in the industry
- job openings
- labor turnover
- union membership and representation
- job gains and losses
- employment by occupation
- projections of occupational employment change
- employer compensation costs
- work-related injuries / fatalities, etc.

B. Education, Skills and Competencies For Better Job Matching

CIORS shall provide information on the education, skills, and competencies (through National Certificate issued by TESDA) of individual construction industry workers including information on other mandatory trainings attended such as the Construction Safety and Health Training.

This information is necessary in determining:

- the necessity of granting entry to foreign workers and professionals for skills and technical know-how not available locally;
- government interventions necessary for a more effective promotion of the corporate exports of construction and related engineering services.

C. Training and Professional Development Program

CIORS shall provide information on industry insights specific to training needs and the available training and certification programs provided by the government

D. One Stop Shop

CIORS will provide integration services so that registration to other government agencies such as the Bureau of Internal Revenue, PhilHealth, PagIBIG and Social Security System can be applied to by the construction worker in a single site.

E. Job Matching

CIORS shall provide a platform to allow job matching between workers and construction companies and shall also provide a market place for insurance coverage for the workers.

CIORS is an ambitious but necessary system that will greatly benefit the construction workers in the Philippines. A critical success factor of the CIORS is in the registration of the workers to own a digital wallet. The digital wallet contains the worker's unique ID and specific information such as skills, competencies, trainings attended and employment history. The wallet will be a secure and permanent asset owned by the new breed of digital workers in the Philippine construction industry.

CMDF is issuing this Terms of Reference as the basis to evaluate suppliers that want to be accredited as Value Added Service Provider (VASP) to provide registration and creation of a blockchain based digital wallet. This will cover Phase 1 of the CIORS project.

The subsequent phases of CIORS shall be procured by public bidding in conformance with RA 9184 in Q1 of 2021.

2. Digital Wallet Portals

2.1. Digital Wallet Portals

- 2.1.1. The VASP shall provide digital wallet portals (DWP) corresponding types of user roles. The functions and features of the portals should include, but not limited to the points listed in the following paragraphs.

The VASP, to be accredited, must show that their existing portals support each of the requirement.

- 2.1.2. The DWP are divided into three parts - the Worker Portal, the CMDF Portal, and the Public Portal. The Worker Portal allows workers to apply for a digital ID and wallet and enter the required information. After their IDs are published, the workers can authorize and share their IDs to parties concerned (in the Public Portal). CMDF portal provides approval/rejection processes and dashboards to management. Employers can use the Public Portal to verify and access the qualification of the workers (anonymized to conform to Data Privacy Laws) with minimal steps. It will also allow employers and the public to use the sponsorship facility.

- 2.1.3. DWP shall cover at least 2 types of IDs:

- Provisional IDs are IDs of workers who may have incomplete information and/or have not fully paid the registration fees and have not been granted accreditation by CMDF.
- Permanent IDs are IDs of workers who have been granted accreditation by CMDF.

2.2. Requirements on User Experiences and Interfaces Design

- 2.2.1. The DPW shall enable a seamless user experience through friendly and intuitive user interfaces.
- 2.2.2. The VASP is required to justify their user experience (UX) design principles and strategy adopted by their system.
- 2.2.3. The VASP shall provide UI and UX showcases of their past projects similar to the services offered.

2.3. Functional Requirements on Account Administration Access Control

The information below describes the required access control for the CMDF portal which aims to have flexibility on the access control management.

2.3.1. Design Requirements

- 2.3.1.1. One Administrative Account shall be configurable with more than one Administrative Role.
 - 2.3.1.2. Each Administrative Role has its own configurable Data Attribute Filter to ensure that sensitive data is accessible only by the authorized User.
 - 2.3.1.3. Each Role shall be configurable for its accessible Functions and Actions for the Administration Portal; New Role shall be allowed to setup without source code change.
 - 2.3.1.4. Functions shall be configurable and grouped by System/Module (i.e., CMDF Admin, etc.) in the Admin Menu. Menu Folder hierarchy shall be enabled.
 - 2.3.1.5. Each Function and Action can be configured as active or disabled.
- 2.3.2. The DWP shall provide a function for Maintaining User Account.
Roles and Data Attribute Filters assigning to User shall be maintained by this function.
- 2.3.3. The DWP shall provide function for Maintaining User Role and Function.
Accessible Functions and Actions by Roles shall be maintained by this function.
- 2.3.4. The DWP shall provide function for Maintaining System, Function and Action.

2.4. Functional Requirements on Worker Portal

2.4.1. Design Requirements on Worker ID and Wallet

- 2.4.1.1. Each worker will have a unique identification number.
- 2.4.1.2. The ID shall be formatted in the following manner: YY-XXXXXXX where YY is the year enrolled and XXXXXXX is the sequence number.
- 2.4.1.3. A worker can have several skills, competencies, certifications and employment history.
- 2.4.1.4. The worker can enter his/her information him/herself using the VASP website.

2.4.1.5. The worker can enter his/her information him/herself using a mobile app.

2.4.1.6. CMDF may also accredit companies to enter the data on behalf of the worker.

2.5. General Design Requirements of CMDF Portal

2.5.1. Users from CMDF shall only be able to maintain and enquire the information of workers based on the Data Attribute Filter configured.

2.5.2. The CMDF Portal shall enable CMDF Users to change their assigned Role from one to another.

2.5.3. All maintenance actions shall be able to perform by batch/bulk and by transaction file import unless otherwise specified.

2.5.4. All functions shall facilitate Search and View Detail action.

2.5.5. All functions shall facilitate Export and Download action.

2.5.6. For all actions involving change(s), notification shall be sent to the recipient specified on the default recipient list in the Notification Template unless otherwise specified, plus other persons as required by CMDF and CIAP.

2.5.7. The CMDF Portal provide a function for Maintaining Worker Information:

It shall enable action(s) to maintain the worker information related to the Worker Portal, such as the Worker ID Merging/Correlation mentioned in Section 2.6.3, etc., if necessary.

2.5.8. The CMDF Portal shall provide function for Uploading Worker Credentials.

2.5.9. The CMDF Portal shall provide function for Verifying Worker Credentials.

- a) It shall include the Verify action, Withdraw action, Revoke action, etc.
- b) It shall indicate the presence of previous version and the configured default handling for further re-issuance preparation, if necessary.

2.5.10. The CMDF Portal shall provide function for Approving Worker Credentials.

It shall include the Approve and Reject actions.

2.5.11. The CMDF Portal shall provide a function for Publishing Worker Credentials.

- a) It shall include the Schedule Publish action, Real Time Publish action, etc.
- b) It shall facilitate simple day calculation logic in UI for configuring the publish date.

2.5.12. The CMDF Portal shall provide a function for Updating Worker Credentials.

- a) It shall include the Withdrawn action, Re-activate action for those Rejected or Withdrawn Credentials, etc.
- b) It shall include the Withdrawn action for withdrawing the upload, revoke, re-issue Worker Credentials request if it is not yet approved or rejected.
- c) The upload, revoke, re-issue actions shall require approval before the Worker Credentials can be published.

2.5.13. The CMDF Portal shall provide a function for Enquiry for Worker information and Credentials.

- a) It shall include the Search action, View Detail action, Download action for ACVP Credentials, Export action for enquiry result, etc.

- b) It shall include search filters which cover most of the data fields. It shall enable User to select the display items for search result for most of the data fields. User shall be able to export the data from the search result (E.g. skills list, etc.). The search filter shall include result with “Latest Version Only” or “All Versions” for selection.
- c) It shall facilitate below report generation actions:
 - List of uploaded records with hash values, publishing duration and preview link of the uploaded PDF files if any, etc.;
 - List of records that fail uploading to the DWP and the reason.

2.5.14. A standalone tool/program shall be provided to:

- a) Generate, encrypt and embed the worker credentials’ metadata into PDF file (i.e. XMP) as worker credentials or if the worker credentials without credentials’ image file, the tool/program shall generate, encrypt and embedding the worker credentials’ metadata into JSON format as worker credentials;
- b) Upload the worker credentials and write the hash value of the worker credentials on the blockchain in batch mode.

2.6. Functional Requirements of Worker Portal

The section describes the functions to be provided to the Worker.

2.6.1. Create Account and Login

- 2.6.1.1. The DWP shall allow Workers to sign-up using the CMDF.
- 2.6.1.2. The DWP shall allow Workers to sign-up using the mobile app.
- 2.6.1.3. The DWP shall allow biometric information as part of the registration process.
- 2.6.1.4. The DWP shall provide a payment facility that allows for online and offline (but automated) payment options.
- 2.6.1.5. During the sign-up process, the Workers shall create their login name and password.
- 2.6.1.6. Workers who cannot authenticate successfully shall be alerted with an error message and will be given instructions accordingly.

2.6.2. Personal Email Address Update

- 2.6.2.1. The Worker Portal shall allow Workers to input and update their email address with verification process.

2.6.3. Worker Account Merging / Correlation

- 2.6.3.1. The Worker Portal shall display (but not limited to) the following worker information:
 - a) Worker’s First Name, Middle Initial, Last Name
 - b) Workers’ Unique Construction ID
 - c) Worker’s Address
 - d) Worker’s Mobile Phone
- 2.6.3.2. The Worker Portal shall allow Workers to update the following information:
 - a) Worker’s First Name, Middle Initial, Last Name

- b) Worker's Address
- c) Worker's Mobile Phone

2.6.4. Qualification Credentials Sharing

- 2.6.4.1. Employers registered through the Public Portal shall be allowed to view anonymized Worker data focused on validated skills, competencies, trainings attended and employment history.
- 2.6.4.2. The full Job Matching facility shall be part of Phase 2 of the CIORS.

2.6.5. Logout

- 2.6.5.1. All Portals (Worker, CMDF and Public Portals) shall automatically logout the users when they are idle for a period of time. The idle period is configurable by the platform administrator at the CMDF Portal.
- 2.6.5.2. The DWP shall automatically logout the previous sessions when the user logs in a new session. The DWP shall not allow concurrent logins.

2.7. Functional Requirements on Public Portal

2.7.1. Basic Functions

- 2.7.1.1. The users of Public Portal are mainly employers, but can also be used by other organizations such as training institutions.
- 2.7.1.2. The Public Portal allows employers to register by using their PCAB ID.
- 2.7.1.3. The Public Portal allows authorized users to view the anonymized credentials of the Worker and can choose specific tasks such as sending hiring notification, displaying filtered information (number of masons in a certain locality),
- 2.7.1.4. The feature to integrate the information from the PCAB site will be part of Phase 2 of CIORS.

2.8. Functional Requirements of Master Data Maintenance

2.8.1. The VASP shall show that the DWP was developed with these principles

- 2.8.1.1. For data with discrete item options, the VASP utilized System Decode for keeping the data in order to leave flexibility for future value change.
- 2.8.1.2. UI text is solely for display only. The VASP did not use it for business decision (e.g. keep server credential, etc.).
- 2.8.1.3. The VASP never performed hard-coding for system sustainability.
- 2.8.1.4. For business decision purpose, VASP referred to the values kept in System Parameter, System Decode or constant.
- 2.8.1.5. For display purpose, the VASP always referred to System Parameter, System Decode or UI text.

2.8.2. The DWP shall provide function for Maintaining UI File.

- 2.8.2.1. The default UI File content could be overridden by CMDF.

- a) E.g. Upload a new logo or graphics.
- b) E.g. System Message html embedded code for CMDF announcement.
- c) E.g. System Message html embedded code for system maintenance message.
- d) The UI File shall provision for different languages.

2.9. Functional Requirements on System Maintenance

- 2.9.1. The DWP shall provide function for Maintaining System Parameter and shall be configurable for the following:
- a) E.g. Parameter for configuring relevant APIs / Smart Contracts credentials (client secret/key/token);
 - b) E.g. Parameter for configuring External Image Server related setting.

2.10. Functional Requirements on API

- 2.10.1. The API authentication shall be identity-based and managed by appropriate Identity & Access Management solution. Acceptable authentication included use of access tokens and refresh tokens based on OAuth v2 as well as account-based API key.
- 2.10.2. CMDF administrators shall be allowed to manage (creation/deletion) the API keys in the portal.
- 2.10.3. The DWP shall provide reports on API usages.
- 2.10.4. The VASP shall provide API online documentations for APIs usable by other agencies institutions and employers.
- 2.10.5. The DWP shall provide below RESTful API for CMDF and other authorized third parties:
- a) Bulk upload of worker information and credentials
 - b) Retrieve the list of worker information and credentials from the DWP with parameters for filtering, such as skills, competencies, etc.
 - c) Bulk download of worker information and credentials
 - d) Bulk validation of worker information and credentials with parameters to specify which credentials to validate (positive or negative)
 - e) Bulk update of worker information credential attributes
 - f) Upload a white list of worker accounts, etc.
 - g) Identity Access Management (IAM) or other authentication mechanisms (i.e. OAuth in JWT format) shall be implemented for authorization
- 2.10.6. For each bulk action, institution shall have the option to specify:
- Commit and save the whole batch only if there is zero error or zero rejected record, or
 - Commit and save for any good records and reject error records.

2.11. Other Functional Requirements on the DWP

- 2.11.1. The CMDF Portal, Worker Portal and Public Portal shall use different URLs for security protection.
- 2.11.2. The DWP shall have its own user repository for maintaining the user profiles.
- 2.11.3. Capacity Requirements
- 2.11.4. The ASP shall provide the resources requirements, including the amount of disk space required, memory required, CPU power and other resources required for the DWP

including the web application server architecture in supporting the expected volume of users and expected response time.

- 2.11.5. The VASP shall provide information in the approach of scaling up the DWP to support additional concurrent users and data volume, both at the back end database level and at the middle-tier application server level. In addition, the DWP shall provide a job scheduling function to handle the peak time demand.
- 2.11.6. The DWP shall provide Private Blockchain network, which issues, stores and verifies the smart contracts and chaincode transactions, to supports the DWP to issue, sign, manage, share, verify, view and download delivering the CMDF from not only JSON and PDF but also via URL link to sign, verify and view the digital CMDF Credentials.
- 2.11.7. The consortium network of the DWP shall be scalable that allow joining or disconnecting dynamically with other Private Blockchain network (i.e. open source or commercial version) and able to re-configure the consensus mechanism for the new joined or disconnected Blockchain networks.
- 2.11.8. The VASP developed smart contracts or chaincode for the CMDF Credentials records on the Private Blockchain network as if issuing, signing, managing, viewing, verifying and sharing of those CMDF Credentials portfolios by URL, QR code or other file format.
- 2.11.9. VASP should be able to provide the option to allow CIAP to host a private blockchain node from the 2nd year onwards.
- 2.11.10. The DWP shall have high reliability and accessibility. The redundancy mechanism of the critical components or functions of the DWP are designed into the Solution with scale-out capability.
- 2.11.11. The DWP shall support the minimum capacity requirements as stated in the table below.

#	User Type	Number of Users
1	DWP Administrator	3
2	CMDF/CIAP Administrator	5
3	Worker	500,000 for the first year
4	Public (i.e. employers)	100,000 for the first year

2.12. Performance Requirements

- 2.12.1. The DWP should achieve response time (i.e. at any time, the client response time for accessing the DWP should be less than expected response time seconds. The client response time is defined as the time taken from the moment the <submit> key is depressed or the mouse is clicked to the time the reasonable response is displayed on the screen of user) according to the followings:

#	Type of Transaction	Expected Response Time
1	Logon to DWP	around 1 second
2	Verify and retrieve worker information	around 3 seconds
3	Create Worker ID	around 5 seconds

- 2.12.2. The VASP shall show that their system conforms to the performance requirement.

3. VASP Eligibility

The VASP must pass the eligibility criteria and show the Minimum Viable Product of their system.

The tables below provide the eligibility criteria and list the required features that must be included in the Minimum Viable Product.

1.0	Eligibility Requirements	Compliance of VASP Applicant (YES/NO)
1.1	Organization Ownership	
1.1.1	Corporations duly organized under the laws of the Philippines, and of which at least sixty percent (60%) of the outstanding capital stock belongs to citizens of the Philippines; OR	
1.1.2	Persons/entities forming themselves into a joint venture, i.e., a group of two (2) or more persons/entities that intend to be jointly and severally responsible or liable for a particular contract: Provided, however , That Filipino ownership or interest of the joint venture concerned shall be at least sixty percent (60%). For this purpose, Filipino ownership or interest shall be based on the contributions of each of the members of the joint venture as specified in their JVA.	
1.2	Legal Documents	
1.2.1	Registration certificate from SEC, Department of Trade and Industry (DTI) for sole proprietorship, or CDA for cooperatives, or sole proprietorship, or CDA for cooperatives.	
1.2.2	Mayor's/Business permit issued by the city or municipality where the principal place of business of the prospective bidder is located, or the equivalent document for Exclusive Economic Zones or Areas.	
1.2.3	Tax clearance per E.O. 398, s. 2005, as finally reviewed and approved by the Bureau of Internal Revenue (BIR).	
1.2.4	If the VASP is a JV, all local members of the JV must submit these documents. For foreign JV partners, the equivalent SEC and Business permit documents from their country (properly notarized by the Philippine Embassy) will suffice as initial submission. The foreign JV partner will have to submit the tax clearance within six (6) months of the start of the service.	
1.3	Technical Documents	
1.3.1	Statement of VASP on blockchain projects for the past three (3) years.	
1.3.2	Statement of VASP on value added service model projects for the past three (3) years.	
1.3.3	Statement of VASP on implemented project that involves biometric (specifically facial recognition) verification that has a scope of at least one million (1,000,000) transactions/facial matches.	

1.3.4	Statement from VASP that storage of data will reside in the Philippines.	
1.3.2	If the VASP is a JV, any member of the JV must submit these documents.	
1.4	Other Documents	
1.4.1	A valid joint venture agreement (JVA), in case the joint venture is already in existence. In the absence of a JVA, duly notarized statements from all the potential joint venture partners should be included in the bid, stating that they will enter into and abide by the provisions of the JVA in the event that the bid is successful.	
1.4.2	If the VASP is a JV, any member of the JV must submit the PhilGEPS Certificate of Registration. Foreign JV partners will need to submit the PhilGEPS Certificate of Registration with six (6) from the start of service.	

In case of foreign bidders, the eligibility requirements or statements, the bids, and all other documents to be submitted to the CMDF must be in English.

All documents submitted must be notarized.

Nothing follows for this section. Next page provides features starting with 2.1

	FEATURE	Minimum Viable Product	Delivered Within 6 Months from the Start of Services	Compliance of VASP Applicant (YES/NO)
2.1	Digital Wallet Portals			
2.1.1	The VASP shall provide digital wallet portals (DWP) corresponding types of user roles. The functions and features of the portals should include, but not limited to the points listed in the following paragraphs. The VASP, to be accredited, must show that their existing portals support each of the requirement.	✓		
2.1.2	The DWP is divided into three parts - the Worker Portal, the CMDF Portal, and the Public Portal.	✓		
	The Worker Portal allows workers to apply for a digital ID and wallet and enter the required information. After their IDs are published, the workers can authorize and share their IDs to parties concerned (in the Public Portal).	✓		
	CMDF portal provides approval/rejection processes and dashboards to management. Employers can use the Public Portal to verify and access the qualification of the workers (anonymized to conform to Data Privacy Laws) with minimal steps.	✓		
	It will also allow employers and the public to use the sponsorship facility.	✓		
2.1.3	DWP shall cover at least two types of IDs:	✓		
	Provisional IDs are IDs of workers who may have incomplete information and/or have not fully paid the registration fees and have not been granted accreditation by CMDF.	✓		
	Permanent IDs are IDs of workers who have been granted accreditation by CMDF.	✓		

	FEATURE	Minimum Viable Product	Delivered Within 6 Months from the Start of Services	Compliance of VASP Applicant (YES/NO)
2.2	Requirements on User Experiences and Interfaces Design			
2.2.1	The DPW shall enable a seamless user experience through friendly and intuitive user interfaces.	✓		
2.2.2	The VASP is required to justify their user experience (UX) design principles and strategy adopted by their system.	✓		
2.2.3	The VASP shall provide UI and UX showcases of their past projects similar to the services offered.	✓		
2.3	Functional Requirements on Account Administration Access Control			
	The information below describes the required access control for the CMDF portal, which aims to have flexibility on the access control management.			
2.3.1	Design Requirements			
	Each Administrative Role has its own configurable Data Attribute Filter to ensure that sensitive data is accessible only by the authorized User.		✓	
	Each Role shall be configurable for its accessible Functions and Actions for the Administration Portal; New Role shall be allowed to set up without source code change.	✓		
	Functions shall be configurable and grouped by System/Module (i.e., CMDF Admin, etc.) in the Admin Menu. Menu Folder hierarchy shall be enabled.	✓		
	Each Function and Action can be configured as active or disabled.	✓		
2.3.2	The DWP shall provide a function for Maintaining User Account.			
	Roles and Data Attribute Filters assigning to User shall be maintained by this function.	✓		
2.3.3	The DWP shall provide a function for Maintaining User Role and Function.			
	Accessible Functions and Actions by Roles shall be maintained by this function.	✓		
2.3.4	The DWP shall provide the function for Maintaining System, Function and Action.	✓		

	FEATURE	Minimum Viable Product	Delivered Within 6 Months from the Start of Services	Compliance of VASP Applicant (YES/NO)
2.4.	Functional Requirements on Worker Portal			
2.4.1	Design Requirements on Worker ID and Wallet			
2.4.1.1	Each worker will have a unique identification number.	✓		
2.4.1.2	The ID shall be formatted in the following manner: YY-XXXXXXX. Where YY is the year enrolled and XXXXXX is the sequence number.	✓		
2.4.1.3	A worker can have several skills, competencies, certifications and employment history.	✓		
2.4.1.4	The worker can enter his/her information him/herself using the VASP website.	✓		
2.4.1.5	The worker can enter his/her information him/herself using the mobile app.		✓	
2.4.1.6	CMDF may also accredit companies to enter the data on behalf of the worker.		✓	
2.5.	General Design Requirements of CMDF Portal			
2.5.1	Users from CMDF shall only be able to maintain and enquire the information of workers based on the Data Attribute Filter configured.		✓	
2.5.2	The CMDF Portal shall enable CMDF Users to change their assigned Role from one to another.	✓		
2.5.3	All maintenance actions shall be able to perform by batch/bulk and by transaction file import unless otherwise specified.	✓		
2.5.4	All functions shall facilitate Search and View Detail action.	✓		
2.5.5	All functions shall facilitate Export and Download action.	✓		
2.5.6	The CMDF Portal provide a function for Maintaining Worker Information: It shall enable action(s) to maintain the worker information related to the Worker Portal, such as the Worker ID Merging/Correlation mentioned in Section 2.6.3, etc., if necessary.	✓		
2.5.7	The CMDF Portal shall provide the function for Uploading Worker Credentials.		✓	

	FEATURE	Minimum Viable Product	Delivered Within 6 Months from the Start of Services	Compliance of VASP Applicant (YES/NO)
2.5.9	The CMDF Portal shall provide the function for Verifying Worker Credentials.			
	a. It shall include the Verify action, Withdraw action, Revoke action, etc.	✓		
	b. It shall indicate the presence of a previous version and the configured default handling for further re-issuance preparation, if necessary.		✓	
2.5.10	The CMDF Portal shall provide the function for Approving Worker Credentials.			
	It shall include the Approve and Reject actions.	✓		
2.5.11	The CMDF Portal shall provide a function for Publishing Worker Credentials.			
	a. It shall include the Revoke action, etc. The mandatory reason is required with a double prompt for confirmation.	✓		
	b. Revoked Credentials shall only be searched or enquired through this function and they shall be hidden from other functions.	✓		
2.5.12	The CMDF Portal shall provide a function for Updating Worker Credentials.			
	a. It shall include the Withdrawn action, Re-activate action for those Rejected or Withdrawn Credentials, etc.		✓	
	b. It shall include the Withdrawn action for withdrawing the upload, revoke, re-issue Worker Credentials request if it is not yet approved or rejected.		✓	
	c. The upload, revoke, re-issue actions shall require approval before the Worker Credentials can be published.		✓	
2.5.13	The CMDF Portal shall provide a function for Enquiry for Worker information and Credentials.			
	a. It shall include the Search action, View Detail action, Download action for ACVP Credentials, Export action for enquiry result, etc.	✓		
	b. It shall include search filters which cover most of the data fields. It shall enable User to select the display items for a search result for most of the data fields. User shall be able to export the data from the search result (E.g. skills list, etc.). The search filter shall include result with "Latest Version Only" or "All Versions" for selection.	✓		

	FEATURE	Minimum Viable Product	Delivered Within 6 Months from the Start of Services	Compliance of VASP Applicant (YES/NO)
	c. It shall facilitate below report generation actions: - List of uploaded records with hash values, publishing duration and preview link of the uploaded PDF files if any, etc.; - List of records that fail to upload to the DWP and the reason.		✓	
2.5.14	A standalone tool/program shall be provided to:			
	a. Generate, encrypt and embed the worker credentials' metadata into PDF file (i.e. XMP) as worker credentials or if the worker credentials without credentials' image file, the tool/program shall generate, encrypt and embedding the worker credentials' metadata into a JSON format as worker credentials;		✓	
	b. Upload the worker credentials and write the hash value of the worker credentials on the blockchain in batch mode.		✓	
2.6	Functional Requirements of Worker Portal			
	The section describes the functions to be provided to the Worker.			
2.6.1	Create Account and Login			
2.6.1.1	The DWP shall allow Workers to sign-up using the CMDF site.	✓		
2.6.1.2	The DWP shall allow Workers to sign-up using the mobile app.		✓	
2.6.1.3	The DWP shall allow biometric information as part of the registration process.		✓	
2.6.1.4	The DWP shall provide a payment facility that allows for online and offline (but automated) payment options.	✓		
2.6.1.5	During the sign-up process, the Workers shall create their login name and password.	✓		
2.6.1.5	Workers who cannot authenticate successfully shall be alerted with an error message and will be given instructions accordingly.	✓		
2.6.2	Personal Email Address Update			
2.6.2.1	The Worker Portal shall allow Workers to input and update their email address with the verification process.	✓		

	FEATURE	Minimum Viable Product	Delivered Within 6 Months from the Start of Services	Compliance of VASP Applicant (YES/NO)
2.6.3	Worker Account Merging / Correlation			
2.6.3.1	The Worker Portal shall display (but not limited to) the following worker information:	✓		
	a. Worker's First Name, Middle Initial, Last Name	✓		
	b. Workers' Unique Construction ID	✓		
	c. Worker's Address	✓		
	d. Worker's Mobile Phone	✓		
2.6.3.2	The Worker Portal shall allow Workers to update the following information:	✓		
	a. Worker's First Name, Middle Initial, Last Name	✓		
	b. Worker's Address	✓		
	c. Worker's Mobile Phone	✓		
2.6.4	Qualification Credentials Sharing			
2.6.4.1	Employers registered through the Public Portal shall be allowed to view anonymized Worker data focused on validated skills, competencies, training attended and employment history.	✓		
2.6.5	Logout			
2.6.5.1	All Portals (Worker, CMDF and Public Portals) shall automatically logout the users when they are idle for a period of time. The idle period is configurable by the platform administrator at the CMDF Portal.	✓		
2.6.5.2	The DWP shall automatically logout the previous sessions when the user logins a new session. The DWP shall not allow concurrent logins.	✓		
2.7	Functional Requirements on Public Portal			
2.7.1	Basic Functions			

	FEATURE	Minimum Viable Product	Delivered Within 6 Months from the Start of Services	Compliance of VASP Applicant (YES/NO)
2.7.1.1	The users of Public Portal are mainly employers, but can also be used by other organizations such as training institutions.		✓	
2.7.1.2	The Public Portal allows employers to register by using their PCAB ID.		✓	
2.7.1.3	The Public Portal allows authorized users to view the anonymized credentials of the Worker and can choose specific tasks such as sending hiring notification, displaying filtered information (number of masons in a certain locality),		✓	
2.8	Functional Requirements of Master Data Maintenance			
2.8.1	The VASP shall show that the DWP was developed with these principles:			
2.8.1.1	For data with discrete item options, the VASP utilized System Decode for keeping the data in order to leave flexibility for future value change.		✓	
2.8.1.2	The DWP shall provide the function for Maintaining UI File.		✓	
2.8.1.3	The VASP never performed hard-coding for system sustainability.		✓	
2.8.1.4	For business decision purpose, VASP referred to the values kept in System Parameter, System Decode or constant.		✓	
2.8.1.5	For display purpose, the VASP always referred to System Parameter, System Decode or UI text.		✓	
2.8.2	The DWP shall provide the function for Maintaining UI File.			
2.8.2.1	The default UI File content could be overridden by CMDF.		✓	
	a. E.g. Upload a new logo or graphics.		✓	
	b. E.g. System Message HTML embedded code for CMDF announcement.		✓	
	c. E.g. System Message HTML embedded code for system maintenance message.		✓	
	d. The UI File shall provision for different languages.		✓	
2.9	Functional Requirements on System Maintenance			

	FEATURE	Minimum Viable Product	Delivered Within 6 Months from the Start of Services	Compliance of VASP Applicant (YES/NO)
2.9.1	The DWP shall provide a function for Maintaining System Parameter and shall be configurable for the following:		✓	
	a. E.g. Parameter for configuring relevant APIs / Smart Contracts credentials (client secret/key/token);		✓	
	b. E.g. Parameter for configuring External Image Server related setting.		✓	
2.10	Functional Requirements on API			
2.10.1	The API authentication shall be identity-based and managed by appropriate Identity & Access Management solution. Acceptable authentication included the use of access tokens and refresh tokens based on OAuth v2 as well as an account-based API key.		✓	
2.10.2	CMDF administrators shall be allowed to manage (creation/deletion) the API keys in the portal.		✓	
2.10.3	The DWP shall provide reports on API usages.		✓	
2.10.4	The VASP shall provide API online documentation for APIs usable by other agencies institutions and employers.		✓	
2.10.5	The DWP shall provide below RESTful API for CMDF and other authorized third parties:		✓	
	a. Bulk upload of worker information and credentials		✓	
	b. Retrieve the list of worker information and credentials from the DWP with parameters for filtering, such as skills, competencies, etc.		✓	
	c. Bulk download of worker information and credentials		✓	
	d. Bulk validation of worker information and credentials with parameters to specify which credentials to validate (positive or negative)		✓	
	e. Bulk update of worker information credential attributes		✓	
	f. Upload a white list of worker accounts, etc.		✓	

	FEATURE	Minimum Viable Product	Delivered Within 6 Months from the Start of Services	Compliance of VASP Applicant (YES/NO)
	g. Identity Access Management (IAM) or other authentication mechanisms (i.e. OAuth in JWT format) shall be implemented for authorization		✓	
2.10.6	For each bulk action, the institution shall have the option to specify:		✓	
	Commit and save the whole batch only if there is zero error or zero rejected record, or		✓	
	Commit and save for any good records and reject error records.		✓	
2.11	Other Functional Requirements on the DWP			
2.11.1	The CMDF Portal, Worker Portal and Public Portal shall use different URLs for security protection.		✓	
2.11.2	The DWP shall have its own user repository for maintaining the user profiles.		✓	
2.11.3	Capacity Requirements			
2.11.4	The ASP shall provide the resources requirements, including the amount of disk space required, memory required, CPU power and other resources required for the DWP including the web application server architecture in supporting the expected volume of users and expected response time.		✓	
2.11.5	The VASP shall provide information in the approach of scaling up the DWP to support additional concurrent users and data volume, both at the back end database level and at the middle-tier application server level. In addition, the DWP shall provide a job scheduling function to handle the peak time demand.		✓	
2.11.6	The DWP shall provide Private Blockchain network, which issues, stores and verifies the smart contracts and chain code transactions, to supports the DWP to issue, sign, manage, share, verify, view and download delivering the CMDF from not only JSON and PDF but also via a URL link to sign, verify and view the digital CMDF Credentials.		✓	

	FEATURE	Minimum Viable Product	Delivered Within 6 Months from the Start of Services	Compliance of VASP Applicant (YES/NO)
2.11.7	The consortium network of the DWP shall be scalable that allow joining or disconnecting dynamically with other Private Blockchain network (i.e. open-source or commercial version) and able to re-configure the consensus mechanism for the new joined or disconnected Blockchain networks.		✓	
2.11.8	The VASP developed smart contracts or chain code for the CMDF Credentials records on the Private Blockchain network as if issuing, signing, managing, viewing, verifying and sharing of those CMDF Credentials portfolios by URL, QR code or other file formats.		✓	
2.11.9	VASP should be able to provide the option to allow CIAP to host a private blockchain node from the 2 nd year onwards.		✓	
2.11.10	The DWP shall have high reliability and accessibility. The redundancy mechanism of the critical components or functions of the DWP is designed into the Solution with scale-out capability.		✓	
2.11.11	The DWP shall support the minimum capacity requirements as follows: a) DWP Administrator - 3 users b) CMDF/CIAP Administrator - 5 users c) Worker - 500,000 for the first year d) Public (i.e. Employers) - 100,000 for the first year.		✓	

	FEATURE	Minimum Viable Product	Delivered Within 6 Months from the Start of Services	Compliance of VASP Applicant (YES/NO)
2.12	Performance Requirements			
2.12.1	<p>The DWP should achieve response time (i.e. at any time, the client response time for accessing the DWP should be less than expected response time seconds. The client response time is defined as the time taken from the moment the <submit> key is depressed or the mouse is clicked to the time the reasonable response is displayed on the screen of the user) according to the followings:</p> <ul style="list-style-type: none"> a) Logon to DWP - around 1 second b) Verify and retrieve worker information - around 3 seconds c) Create Worker ID - around 5 seconds. 		✓	
2.12.2	The VASP shall show that their system conforms to the performance requirement.		✓	