GOVERNMENT OF
WESTERN AUSTRALIA

Addendum to Request Documents

Request No.: DPC2142

Addendum No.: 3

Date of issue: 01 September 2025

No. of pages: 5

Important

By submitting an Offer, a Respondent will be deemed to have reviewed and understood this Addendum.

Addendum Advice

Item 1	
Reference	5. Qualitative Requirements b). Suitability of Proposed Approach and Methodology
Query	Are testing staff required to be on-site at the designated DPC location or can testing be delivered remotely.
Response	The testing strategy will be discussed and agreed during contract negotiation based on material provided by the preferred respondent/s.

Item 2	
Reference	5. Qualitative Requirements b). Suitability of Proposed Approach and Methodology
Query	Does the Department have an existing test management, i.e., JIRA, DevOps, tool that is preferred for use during UAT and other testing activities.
Response	The specific test activities that will be run and what is required of the Contractor will be discussed and agreed during contract negotiations.

Item 3	
Reference	5. Qualitative Requirements b). Suitability of Proposed Approach and Methodology
Query	Is there Departmental level test strategy respondents needs to align with for completion of testing for the new service, and if so, can this be shared.
Response	Pilot integration and end to end test activities (including what is required of the Contractor) will be discussed and agreed during contract negotiations.

Item 4	
Reference	Schedule 2 - Statement of Requirements
Query	Are all in-life management contractual and security requirements required during the Pilot phase?
Response	The staged approach desired based on information sensitivity will be discussed during contract negotiations with the preferred respondent/s.

Item 5	
Reference	Schedule 2 - Statement of Requirements
Query	What is planned in terms of an OEM wallet availability for the Restricted stage?
Response	The Pilot 'Restricted Stage' will validate interoperability with OEM wallet issuing and update standards including OID4VCI as per the Request document.

Item 6	
Reference	Schedule 2 - Statement of Requirements
Query	It is unclear in the architecture as to who would be responsible for the core credential enrolment and issuance journeys which would likely be specific to each agency. Assumption is that the contractor is not required to build bespoke journeys or custom integration (contractor is responsible for the overall orchestration and credential lifecycle management where other parties can plug in)
Response	DGov will develop and manage custom integrations based on material provided by the Contractor. Integration code & workloads will be managed by DGov utilising delegated access to the Wallet SaaS.

Item 7	
Reference	Schedule 2 - Statement of Requirements
Query	Will the integration code that accesses the data sources be permitted to be installed in the ServiceWA existing tenancy or should the vendor establish a new tenancy.
Response	DGov will develop and manage custom integrations based on material provided by the Contractor. Integration code & workloads will be managed by DGov utilising delegated access to the Wallet SaaS.

Item 8	
Reference	Schedule 2 - Statement of Requirements
Query	What is the rationale for using the term Wallet SaaS instead of Credential Issuance Platform?
Response	The term 'Wallet SaaS' was used to indicate that the credential issuance platform shall be delivered as-a-Service.

Item 9	
Reference	Schedule 2 - Statement of Requirements
Query	Are you specifically seeking a custodial wallet solution?
Response	The credential issuance platform shall be delivered as-a-Service and comply to the required standards as specified in the Request documents.

Item 10	
Reference	Schedule 2 - Statement of Requirements
Query	In the architecture diagrams, third-party verifiers are shown integrating with the Wallet SaaS. What is the intended outcome of this integration? Is the Wallet SaaS expected to provide claims? Why is there no interaction between the third-party verifier and the Services WA application?
Response	Third parties are expected to integrate via digital trust services defining lists of issuer and verifier certificates. The SaaS platform is expected to provide trust services to publish certificate authority lists.

Item 11	
Reference	Schedule 2 - Statement of Requirements
Query	In Figure 5, the wallet record contains both a wallet identifier and managed keys. Could you clarify what these managed keys refer to—are they wallet keys or issuer keys?
Response	The managed keys refer to the supplier-provisioned wallet key.

Item 12	
Reference	Schedule 2 - Statement of Requirements
Query	What is the role of Format Credential as shown in Figure 5 and Figure 6?
Response	It represents the conversion/translation from source attributes (in a system of record) into a format aligned to a wallet credential (wallet format).

Item 13	
Reference	Schedule 2 - Statement of Requirements
Query	Regarding revocation, are we required to strictly follow the flows illustrated in Figures 5 and 6, or would it be acceptable to propose an alternative revocation flow?
Response	It is acceptable to propose an alternative revocation flow.

Item 14	
Reference	DPC2142 Attachment 3 - Schedule 3 – Specifications
Query	Can we confirm that an IACA PKI solution (SaaS-based) will need to be provided & managed by the vendor

Item 14	
Response	As per the tender documents, this is correct.

Item 15	
Reference	DPC2142 Attachment 3 - Schedule 3 - Specifications
Query	Can you please confirm that you seek the supplier to provide and maintain all listed security certifications and assessments (IRAP, SOC2, 27001) or only one is sufficient, e.g. ISO 27001? For IRAP assessment, do you require the supplier to support DCP IRAP audit with evidences or you require the supplier service to be IRAP assessed on its own?
Response	The supplier should provide and document the security certifications and assessments (including any statements of applicability) in place for in-scope services. The supplier may provide a roadmap for future certifications and a rationale for certifications not maintained. It is not mandatory that all listed certifications are held, however the supplier must demonstrate compliance with an independent certification process. Responses will be evaluated on the information provided.

Item 16	
Reference	DPC2142 Attachment 3 - Schedule 3 - Specifications
Query	Could you confirm if "customers" are referring to issuers, relying parties, or something else?
Response	For PRM-1 “customers” refers to issuing authorities.

Item 17	
Reference	DPC2142 Attachment 3 - Schedule 3 - Specifications
Query	Could you clarify the expectations for SDK and platform API? We see two aspects of OpenID4VP: 1) Enable the user to share credential with a Relying party / Verifier. Provide issuer-related services to ensure the credential valid. 2) Enable Relying parties to verify a digital document from WA or other standard-compliant wallet Do you want the bidder to provide the verification capability in addition to the wallet sharing?
Response	This is correct, as per the Request documents.

Item 18	
Reference	Schedule 2 - Statement of Requirements
Query	We would like to confirm WA DGov’s requirements for verification capabilities during both the pilot and production phases. We note the reference to a third-party verifier and the need to support both in-person and remote verification.

Item 18	
	Could we clarify the expectations of the contractor in this regard? Specifically: • Should the contractor propose remote verification capabilities (e.g., SDKs and related components that can be embedded within a website or business application)? • Are SDKs also required to support in-person presentation (e.g., integration into a mobile verification application)? If the contractor is expected to provide this capability, we would appreciate further detail on the intended scope of usage during production. For example, does WA DGov plan to develop a Mobile Verification Application? If so, what is the anticipated scope of use—for instance, which credentials will be supported for verification, and will the application's availability be limited to Australia?
Response	Yes, respondents should propose remote verification capabilities and SDK's for in-person presentation. Anticipated scope is expected to align with the Australian Digital ID Act 2024 and the European Digital Identity Regulation (Regulation (EU) 2024/1183), also known as eIDAS 2.0.

Item 19	
Reference	Schedule 2 - Statement of Requirements – Figures 5 and 6.
Query	Please confirm the vendors are required to complete the integration between the Agency Object Store and our (COTS) wallet platform, with reference to the diagrams provided in Figures 5 and 6 of Attachment 2.
Response	DGov will develop and manage custom integrations based on material provided by the Contractor. Integration code and workloads will be managed by DGov utilising delegated access to the Wallet SaaS.

END ADDENDUM