GOVERNMENT OF WESTERN AUSTRALIA

Addendum to Request Documents

Request No.: DPC2142

Addendum No.: 1

Date of issue: 19 August 2025

No. of pages: 3 (inc. this sheet)

Important

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

Addendum Advice

Item 1	
Reference	Schedule 2 – Specification/Statement of Requirements – Section 1.3 Quality Standards
Query	For each of the referenced ISO standards, could you explicitly state whether full certification is mandatory prior to contract award, or if demonstrable alignment and a clear timeline for achieving full certification post-award will suffice?
Response	Full certification is preferred; however, it is not mandatory for a response. Please refer to the guidelines below for further clarification. For the management system/process related ISO standards like ISO 9001 and ISO 27001, current certification is preferred as it demonstrates organisation and process maturity. In cases where certification has not yet been achieved, Respondents are requested to outline their status within the certification process (e.g., gap analysis, implementation, audit, or specific certification stage) and provide a timeline indicating their intent towards full certification. For interoperability and mobile driver's licence readiness, full ISO 18013-5 certification is preferred, ideally issued by a recognised body such as UL Solutions. In the absence of full certification, a clear timeline and risk analysis would suffice for the tender response. Where the ISO standards is more of a technical framework, an internally validated self-assessment is sufficient with accompanying detailed documentation. Regardless of current certification status, Respondents should provide a clear and detailed explanation of their position and work in progress, or future intentions. All responses will be evaluated on its merits.

Item 2	
Reference	Schedule 2 – Specification/Statement of Requirements – Section 1.3 Quality Standards
Query	If a timeline for achieving full certification is acceptable for certain ISO standards, what are the Department's expectations for this timeline (e.g.,

Item 2	
	within 6 months, 12 months, etc., of contract commencement) specific to each ISO standard?
Response	Given that Pilot activities are anticipated to commence in the second quarter of 2026, and any contract extensions (if exercised) would begin in 2027, it is mandatory that the full certification for applicable ISO standards be in place by the end of the Pilot period.

Item 3	
Reference	Schedule 3 - Specifications
Query	Regarding requirements such as "Provide independent test results" or "Provide conformance test results", could you confirm if these refer exclusively to audits and results from accredited third-party organisations, or if internal conformance testing and self-assessments would also be considered as evidence of "progress towards achieving compliance" in the interim?
Response	In the first instance (where certification has not been achieved), a detailed self-assessment would suffice. In line with our response to question 1 above, where certification can be attained for a standard, results from a third-party organisation would be required to prove full certification where applicable.

Item 4	
Reference	Schedule 2 – Specification/Statement of Requirements – Section 1.3 Quality Standards
Query	Given the requirement to "maintain" certifications for the duration of the contract for certain standards like ISO/IEC 27001, could you provide guidance on the frequency and type of ongoing evidence (e.g., annual audits, continuous monitoring reports) expected to demonstrate this maintenance?
Response	Ideally this would be dictated by the requirement of the applicable standard. Guidelines as follows: mDL Standards (18013-5 & 18013-7): While ISO itself does not issue certificates for these, third-party conformity assessments exist for 18013-5. The newer 18013-7 is currently a technical specification and does not yet have formal certification path. Management System Standards (27001, 9001): These are certifiable via accredited bodies, with well-established audit cycles and maintenance requirements. Technical Frameworks (23220-1, 12207, 29100): Do not support formal certification, though can self-assess and align their internal procedures accordingly. Cryptographic Module Standard (19790:2025): Certification isn't ISO-issued but handled through private certification schemes, ensuring ongoing module security validation.

Item 5	
Reference	Schedule 2 – Specification/Statement of Requirements
Query	Would a proposal be accepted if it used existing WA infrastructure and was managed as a managed service instead of SaaS offering?’
Response	If a proposal suggested using existing WA infrastructure and was managed as a managed service instead of a SaaS offering it would be considered.

END ADDENDUM

GOVERNMENT OF WESTERN AUSTRALIA

Addendum to Request Documents

Request No.: DPC2142

Addendum No.: 2

Date of issue: 27 August 2025

No. of pages: 1 (inc. this sheet)

Important

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

Addendum Advice

Item 1	
Reference	Schedule 2 – Specification/Statement of Requirements
Query	Is it correct to assume the implementation of a citizen digital onboarding solution with integrated Know Your Customer (KYC) functionality is outside the main scope of delivery? Is this an optional element you are interested in understanding more about?
Response	Not at this time. KYC is out of scope.

Item 2	
Reference	Schedule 2 – Specification/Statement of Requirements
Query	For the optional biometric matching line item referenced on the financial response, could you kindly provide more information about what is required and how this will be used? It would be really useful to receive further clarification on the expected features, compliance standards, and integration requirements associated with this solution. For example, is there any biometric authentication requirement for 1:1 matching and Liveness detection needed for this optional biometric matching?
Response	Biometrics are not currently in-scope; however, we wanted to provision for it for potential future capability. Noting that all financials can be discussed and refined during negotiation activities for the preferred respondent, at this time, please assume biometrics are to align with Digital ID 2024 data standards Auth Level 2.

Item 3	
Reference	Schedule 2 – Specification/Statement of Requirements
Query	We would like to check if DPC would provide the Contractor the secure room to install the Root CA HSM, Root Key Management System and its Infrastructure which is generally a secure PC?
Response	DPC will manage the Root CA infrastructure.

END ADDENDUM

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

GOVERNMENT OF WESTERN AUSTRALIA

Addendum to Request Documents

Request No.: DPC2142

Addendum No.: 4

Date of issue: 02 September 2025

No. of pages: 2

Important

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

Addendum Advice

Item 1	
Reference	Schedule 12 – Approved Form of Bank Guarantee
Query	*"Unconditionally and irrevocably covenants to pay to the Customer on first demand by the Customer any sum or sums which may from time to time be demanded by the Customer up to an aggregate maximum of [$500,000]."* This wording seems quite strict, and we're trying to better understand under what scenarios the department would seek to enforce the guarantee and require payment, particularly given that insurance is typically intended to cover such risks. Could you please advise whether there is scope to depart from this requirement, or if compliance with this clause will be mandatory?
Response	The inclusion of the Bank Guarantee will be determined with the Preferred Respondent during negotiations. Respondents can propose departures from the Terms and Conditions in their Response. Refer to section 4(a) of DPC2142 Request – Provision of a Digital Wallet and Verifiable Credentials Solution.

Item 2	
Reference	Schedule 2 - Statement of Requirements - 1.4 Proof-of-Operation
Query	Can we confirm if the Supplier PKI can be a test PKI for Proof-of-Operation?
Response	It is acceptable for Supplier PKI to be used as test for Proof-of-Operation.

Item 3	
Reference	Schedule 2 - Statement of Requirements - 1.4 Proof-of-Operation
Query	Can DPC provide a timeline estimate of when the Proof-of-Operation is likely to start? E.g. 1st of Dec?
Response	The Proof-of-Operation is expected to commence in late October. Shortlisted Respondents will be given three weeks from the commencement date to prepare the Proof-of-Operation. A demonstration

Item 3	
	may be required at the end of the three weeks before the two-week assessment by DGov commences.

Item 4	
Reference	Schedule 2 - Statement of Requirements - 1.5 Pilot Phase - 1.5.1 Key Objectives
Query	Can you confirm that “integration with WA Identity exchange” is for the authentication of administrative users from Service WA and issuers, and not for end-users holding wallets.
Response	As per the functional requirements, the platform must be configurable to use standalone OIDC or SAML identity providers for credential workflows. Integration is required from the perspective of supporting OID4VCI workflows as the Identity Exchange sits in the middle of this flow acting as the federated authentication source for issuers.

Item 5	
Reference	Closing Time: 2:30pm Friday 12 September 2025, Western Australia
Query	Can DPC provide a 1-week extension to the closing time/date to Friday September 19th?
Response	Due to the project timelines the closing date cannot be extended.

Note: Please see section 1.5.1 Deadline for Questions in DPC2142 Request - Provision of a Digital Wallet and Verifiable Credentials Solution.

END ADDENDUM

GOVERNMENT OF WESTERN AUSTRALIA

Addendum to Request Documents

Request No.: DPC2142

Addendum No.: 5

Date of issue: 03 September 2025

No. of pages: 1

Important

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

Addendum Advice

Item 1	
Reference	Schedule 2 – Statement of requirements
Query	What is the level of importance / significance attached to the ISO standards specifically related to policy process and procedure only within a response.i.e. adherence to ISO 27001, 9001, 12207, 29100, 19790?
Response	Certification or alignment with the aforementioned ISO standards are indicative of an organisation's level of maturity and demonstrate consistency, process and quality regarding their procedures, information security, and product development. All responses will be considered equally based on the criteria and requirements outlined in the Request and considered and evaluated fairly and consistently as part of each Respondent's overall submission.

END ADDENDUM

GOVERNMENT OF WESTERN AUSTRALIA

Addendum to Request Documents

Request No: DPC2142

Addendum No: 6

Date of issue: 05 September 2025

No. of pages: 3

Important

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

Addendum Advice

Item 1	
Reference	DPC2142 Attachment 2 - Schedule 2 - Statement of Requirements
Query	What scope would you like to see covered by the SaaS hosting fees in the financial response? Are we expected to include the cost of hosting a dedicated instance of the SaaS solution? Or can it be shared with other customers (assuming appropriate logical and physical security and data separation is applied)? If the SaaS solution can be shared with other customers, do you want only the hosting costs attributed to yourselves to be shown in the financial response?
Response	SaaS hosting design and associated costs should be defined by the Respondent. Your proposal should clearly articulate your solution and be costed accordingly.

Item 2	
Reference	DPC2142 Attachment 2 - Schedule 2 - Statement of Requirements
Query	Could you kindly explain what type of multi-tenancy and isolation of data you require for the Issuance Platform? Is logical separation sufficient? Or do you require physical separation with separate infrastructure for each WA end customer? This is important to understand the costs.
Response	SaaS hosting design should be defined by the Respondent. Your response should clearly articulate your proposed solution and be costed accordingly.

Item 3	
Reference	DPC2142 Attachment 2 - Schedule 2 - Statement of Requirements
Query	In order to help us to prepare the best and most economical hosting costs, can you kindly provide some guidance on how you would like us to size the infrastructure during the Pilot phase? For example, is it okay to assume this will be based on the small-scale deployment model? Is there the need for the high availability of all components? Would it be acceptable for the Pilot preproduction environment to operate as a scaled down version of the production environment without the costs of full redundancy (high availability)? Do the SLA availability requirements apply during the pilot phase? Is there the need for disaster recovery during the pilot phase?

Item 3	
	Could you kindly provide more information to help ensure all vendor responses are scoped and costed similarly?
Response	Service delivery is at the discretion of the Respondent. The staged Pilot should be scalable and able to demonstrate the full functionality of the solution in accordance with the Specification and Statement of Requirements.

Item 4	
Reference	DPC2142 Attachment 2 - Schedule 2 - Statement of Requirements
Query	Furthermore, could you also confirm whether, during the full Production phase, the Full Pre-production environment may operate as a scaled-down version of the Full Production environment during periods of inactivity?
Response	Please refer to the Specification and Statement of Requirements.

Item 5	
Reference	DPC2142 Attachment 2 - Schedule 2 - Statement of Requirements
Query	Could you kindly confirm how many environments you require for each stage of the project? For example, we understand the pilot phase will run on the preproduction environment. Can we agree to limit it to just this to reduce the hosting costs during the pilot phase? Can you confirm how many environments you are expecting during the pilot and full production phases? Do they have any specific requirements in terms of sizing for the costing exercise?
Response	Please refer to the Specification and Statement of Requirements.

Item 6	
Reference	DPC2142 Attachment 2 - Schedule 2 - Statement of Requirements
Query	If the infrastructure will be dynamically created or scaled over time, how would you like to scope the hosting costs over time? Can you provide a more detailed production forecast to help us understand how the solution will grow over time?
Response	Hosting costs should be prepared in accordance with the Attachment 4 – Schedule 7 Pricing schedule. For details on Full Production please refer to the Specification and Statement of Requirements.

Item 7	
Reference	DPC2142 Attachment 2 - Schedule 2 - Statement of Requirements
Query	Could you kindly confirm if the SaaS vendor is only expected to provide the Digital Trust Services to support the verifiers? Or should they also provide full OpenID4VP backend verification functionality? We essentially want to understand if the OpenID4VP backend verification functionality will be provided by other third-parties or if the SaaS vendor needs to provide OpenID4VP functionality on the backend that implements the OpenID4VP verification protocol, receives the data from the mobile and exposes it via an APIs to such third-party integrators?

Item 7	
Response	In accordance with Attachment 3 – Schedule 3 Specifications, requirement TS-8, platform presentation APIs and SDKs must adhere to the OpenID for Verifiable Presentations (OID4VP) workflow.

Item 8	
Reference	DPC2142 Attachment 2 - Schedule 2 - Statement of Requirements
Query	Is high availability required for the pilot phase?
Response	As per the specification and Statement of Requirements, the staged Pilot will be scalable and able to demonstrate the full functionality of the solution.

Item 9	
Reference	DPC2142 Attachment 2 - Schedule 2 - Statement of Requirements
Query	Shall WA implementation be dedicated to WA or could it be hosted with other customers?
Response	Hosting design should align with the Respondent's proposed solution. The Response should clearly articulate your solution in accordance with the Specification and Statement of Requirement.

END ADDENDUM