「令和5年度 個人向け認証アプリケーションの開発」調達仕様書に対する意見・質問について

連番	意見内容					デジタル庁回答
	質問／意見	頁	項目名	意見・質問等	理由（意見の場合のみ記述）	
1	質問	10	調達仕様書 (2) バックエンド開発 業務	「モバイルアプリケーション開発チームで発生した必要な変更を吸収する工程をスケジュール作成時には考慮すること」とあります。 仕様書P6で示された作業スケジュールでは、8－9月、10－12月に改修・テストの工程が描かれておりますが、こちらの工程は上記の「必要な変更を吸収する工程」にあたりますでしょうか。		改修・テスト工程が主になります。
2	質問	11	調達仕様書 モバイルアプリ ケーション 及びバックエンド開発共通 参考情報	「評価に当たっては、ページからの離脱率や入力したデータのエラー率など定量的に評価できる機構を用意し、作業完遂率や推定作業時間などの評価軸を設定の上継続的に評価・改善を行えるようにすること」とありますが、Googleアナリティクスの導入で対応することも可能と考えてよろしいでしょうか。		受託者とデジタル庁担当者で議論の上、決定できればと考えます。
3	質問	11	調達仕様書 モバイルアプリ ケーション 及びバックエンド開発共通 参考情報	チケット管理はJIRAとGithubを使用すると記述がありますが、Backlogは対象外でしょうか。		JIRAとGithubを希望します。
4	意見	13	調達仕様書 利用者マニュアルの作成	「利用者マニュアルの作成」とあるが、スマホアプリの操作マニュアルを指すのでしょうか？ スマホアプリのマニュアルを指すのであれば、作業としては、個人認証サービススマホアプリ（モバイルアプリケーション）のテスト・デザイン支援業務（準委任）にて作成する方が効率的と思われます。	利用者の操作は、スマホアプリから行われるため、デザインやテストの担当者の方が効率的に作成できるのではないか、と思います。	スマホアプリの操作マニュアルではなく、バックエンドで開発したシステムのマニュアルです。
5	質問	16	調達仕様書 ② バックエンド開発業務	「17. 欠陥報告書」について。 報告基準、報告タイミング、報告内容などの想定があれば提示いただけないでしょうか。		テスト中を想定しています。
6	意見	21	調達仕様書 (2) 契約不適合責任に関する事項	「キ 前項の規定により、種類又は品質に関する契約不適合に関し履行の追完を請求するには、その契約不適合の事実を知った時から1年以内に受託者に通知することを要する。」について、 以下のとおり変更をお願いできないでしょうか？ 「キ 前項の規定により、種類又は品質に関する契約不適合に関し履行の追完を請求するには、当該案件の契約検収を行ってから1年以内に受託者に通知することを要する。」	一般的なソフトウェアの瑕疵期間は、お客様の検収を受領してから1年となるため。	責任期間を具体的に定めることはいたしかねます。
7	質問	24	調達仕様書 8 その他特記事項	以下の資料が含まれていないため共有をお願いします。 ・別紙3「調達仕様書に盛り込むべき情報資産管理標準シートの提出に関する作業内容」		デジタル・ガバメント推進標準ガイドラインをご参照ください。
8	質問	28	調達仕様書 情報セキュリティに関する事項	以下の資料が含まれていないため共有をお願いします。 ・別紙5「クラウドサービス_ISMAP管理策基準」		別紙名を修正いたしました。「（参考）クラウドサービス_ISMAP管理策基」をご参照ください。 https://www.digital.go.jp/resources/standard_guidelines/
9	質問	4	別紙2_想定する開発体制案及び必要ツール一覧	デプロイツールにはJIRAと記載があるが確定事項でしょうか。Jenkins利用前提でのJIRA利用を想定しているのでしょうか。		未定です。
10	質問	1	別紙3_機能一覧表 利用者証明用電子証明書を用いたmTLSクライアント認証機能	個人認証サービスアプリとの間で二要素認証によるmTLS認証とありますが、PIN(知識)+マイナンバーカード(物理)にて二要素認証になっているという理解で合っていますでしょうか。		ご理解のとおりです。マイナンバーカードを所有していること(Something You Have の SYH)＋PINを知っていることで利用者証明用電子証明書を利用できる(Something You Know の SYK) によって、二要素認証になっているという理解です。
11	質問	1	別紙3_機能一覧表 利用者証明用電子証明書を用いたmTLSクライアント認証機能	mTLSによるクライアント認証を実現するためには、「個人認証サービスアプリ」の機能において、「マイナンバーカードに格納されているJPKI の提供する利用者証明用電子証明書を用いたmTLS」に対応することが必要と考えますが、「個人認証サービスアプリ」の機能において本機能を有する説明がありません。 アプリが同機能を有すると想定しますが認識が合いますでしょうか。 あっている場合はアプリに同機能を有することを明記いただけますでしょうか。		ご理解のとおりです。 本調達からモバイルアプリ開発業務を本調達から削除したため記載はしません。
12	質問	1	別紙3_機能一覧表 利用者証明用電子証明書を用いたmTLSクライアント認証機能	「個人認証サービスアプリ」が、「マイナンバーカードに格納されているJPKI の提供する利用者証明用電子証明書を用いたmTLS」に対応するためには、実装方法によっては（不可能である）マイナンバーカードの秘密鍵の読み出しが必要となります。 「個人認証サービスアプリ」の開発は、調達仕様書の記述から貴庁にて実施されると認識しておりますが、アプリにて本機能の開発・実装は可能とご認識でしょうか。開発可能な場合、それは動作確認済みでしょうか。 テストの対応量を検討するうえで把握したい情報となります。		マイナンバーカードの IC Chipに格納されている秘密鍵を読み出して Chipの外に出すことはありません。Chip内に秘密鍵を保持したまま秘密鍵を利用して APDUコマンドによりハッシュ値を暗号化する処理を行います。その library関数はデジタル庁で開発します。従って、クライアント側は、デジタル庁で開発し動作検証を行う前提で御見積もりいただいて大丈夫です。
13	質問	1	別紙3_機能一覧表 証明書パス検証機能	ユーザ認証APIを新規作成する想定です。 以下を実施し、認証結果を返却する想定ですが認識が合いますでしょうか。 ・#3パス検証 ・#4有効期限検証 ・#7CRL失効確認 ・#13OCSP失効確認 （CRLとOCSPいずれを利用するかはパラメータにて指定） ・ID管理DBにシリアル番号が登録済かのチェック		想定としては合っています。一方、他にも IdP として必要な処理も発生しうるため、詳細は設計時に協議させてください。
14	質問	1	別紙3_機能一覧表 失効情報取得機能（利用者証明用電子証明書）	利用者証明書CRL取得バッチと合わせて、認証局証明書・ARL取得バッチを新規作成する想定ですが、認識が合いますでしょうか。 (パス検証に必要と考えます)		こちらは、新規開発というよりも CRL取得バッチ及び ARL取得バッチ等は、実績のあるマイナポータル（開示システム）の開発物を流用することを想定しています。本仕様に関しては、詳細設計時に仕様を指定することとします
15	意見	1	別紙3_機能一覧表 失効情報取得機能（利用者証明用電子証明書）	「署名用電子証明書のCRLダウンロード機能は、本調達以前に実装済みである」とありますが、実装されていない認識です。	CRLダウンロード機能は本調達以前に実装されていない認識であるため。	実装の参考にするための機能として実装されている、という意味で記載させていただいております。

「令和5年度 個人向け認証アプリケーションの開発」調達仕様書に対する意見・質問について

連番	意見内容					デジタル庁回答
	質問／意見	頁	項目名	意見・質問等	理由（意見の場合のみ記述）	
16	質問	2	別紙3.機能一覧表 ログイン時のトークン発行機能	"amr相当"と記載がありますが、amrクレームを指しているという理解で合っていますでしょうか。		ご理解のとおりです。詳細設計時に amr クレームで表現できない可能性を考慮して、「相当」と記載させていただいています。
17	質問	3	別紙3.機能一覧表 OCSP連携機能を用いた新旧紐付け管理機能	ユーザ登録APIを新規作成する想定です。 以下を実施し、認証結果を返却する想定ですが認識が合いますでしょうか。 ・#3パス検証 ・#4有効期限検証 ・#15 OCSP新旧紐づけ確認 ・有効の場合、ID管理DBに新規登録 ・失効かつ旧シリアル番号が返却されID管理DBに登録済の場合、新シリアル番号に更新 ・上記以外の場合エラー		詳細に記載します。以下の処理を実装していただくことを想定しています。 ユーザ登録APIを作成するというよりも認証処理の延長で、新シリアル番号が ID管理の検索でヒットしなかった場合、OCSP新旧紐付け管理機能により旧シリアル番号を新シリアルに書き換える機能です。 (1) 証明書のパス検証　利用者証明用電子証明書が JPKI認証局から発行された電子証明書であることを検証する。 (2) 有効期限切れの確認 これは既にクライアント側でも行っていますが、念のためサーバー側でも double checkしていただく処理で問題ありません。 (3) ID管理に当該シリアル番号が登録されているか？登録されていない場合は、⇒(4) の処理となります。登録されている場合は、正常処理です。 (4) シリアル番号が登録されていない場合、OCSPの新旧紐付け確認の APIで、新シリアル番号に対応する旧シリアル番号をOCSP Serverに問合せます。問合せの結果、旧シリアル番号が返却された場合、旧シリアル番号を保存した後、ID管理の利用者情報にある旧シリアル番号を新シリアル番号に書き換えます。 (5) OCSP Serverに問合せした結果、旧シリアル番号が返却されなかった場合は登録されていない状態と判定し、認証処理はエラーで復帰値を返却します。
18	質問	3	別紙3.機能一覧表 利用者登録・更新機能（識別子付番及び新規登録紐付け機能）	「利用者から個人認証サービスへの新規登録」とありますが、1枚のマイナンバーカード保持者が、法人の代表者でもあり、個人事業主でもあるケースや個人事業主が複数の事業を営み、RPにおいて各々でアカウントを作成しているケースなどが想定されますが、個人認証サービス側ではRPにおける複数アカウントを見分ける手段がないため、1RPに対して1アカウントに紐づけることになると理解しますが、認識は合致しておりますでしょうか。		ご理解のとおりです。本システムはマイナンバーカード保有者を識別する仕組みを提供することを目的としており、RP側での複数アカウントへの対応は本システムの範囲外となります。
19	質問	3	別紙3.機能一覧表 利用者登録・更新機能（識別子付番及び新規登録紐付け機能）	利用者更新の契機は新旧紐づけ確認後のシリアル番号変更以外にも想定されていますでしょうか？ あれば実行者や呼び出し元、契機の想定を教えてください。		本調達時点では新旧紐付け以外の更新は想定していません。
20	質問	3	別紙3.機能一覧表 登録者削除機能	利用者削除の実行者や呼び出し元、契機の想定を教えてください。API提供や管理機能からの削除などを想定しています。		利用者本人によるアカウント削除を想定しています。 管理者からのアカウント削除は想定していませんが、アカウントの一時停止機能などは必要となる可能性があり、設計時に協議の上で決定するものとします。
21	質問	3	別紙3.機能一覧表 アカウント無効化機能	利用者証明用証明書の失効確認のタイミングで、失効理由CRLReason が affiliationChanged（組織情報の変更）であればID管理DBで無効化する 想定でよろしいでしょうか。		CP/CPSでも affiliation Changed は、利用者証明用電子証明書の記載内容に変更が生じた際の失効事由の一つであること規定が明記されていますので、失効でID管理で無効化する想定でOKです。本仕様に関しては、詳細設計時に再確認します。
22	質問	3	別紙3.機能一覧表 属性情報提供機能	UserInfo エンドポイントは個人認証サービスシステム(バックエンド)を想定します。 4情報が「個人認証サービスアプリ」から、個人認証サービスシステム(バックエンド)に連携されるのはフロー上でどのタイミングになりますか？業務フロー上に明記いただけますでしょうか。		基本設計時に検討とします。
23	質問	3	別紙3.機能一覧表 属性情報提供機能	UserInfo エンドポイントはRP側から有効なアクセストークンが提供される限り、RPから任意のタイミングで呼び出しを受けると想定しますが、認識は合っていますでしょうか。 特定のタイミングを想定される場合は、業務フロー上に明記いただけますでしょうか。		認可コードグラントフローを介して取得した、アクセストークンでのみの提供を想定しています（リフレッシュトークンにて取得したアクセストークンを用いた場合、当該情報は取得できない、といった仕様で考えています）。 詳細は基本設計時に検討とします。
24	質問	3	別紙3.機能一覧表 RP識別子紐付け登録機能	RP識別子紐付け登録APIを新規作成し、指定された利用者に対し登録済RP識別子を登録するまたは認可サーバとのID管理DBを共有する想定です。 業務フローp21でIDPサーバが発行した利用者識別子(仮名)は業務フローp22でRPのID管理DBを参照するタイミングでは必ず未登録になると思われますため、必ず既登録判定はNoとなる想定ですが、認識は合いますでしょうか。 Yesとなるケースがあれば教えていただけますでしょうか。		機能として記載しましたが、本機能はRPにて既存の認証の仕組みを用いてログイン状態となった上で、本システムに対して一般的にな認可フローを実施して、RPにて紐付けを行う形を想定しています。
25	質問	3	別紙3.機能一覧表 識別子紐付けバッチ登録機能	利用者識別子紐づけバッチを新規作成する想定です。 実行者や実行方法(自動/手動)(画面/コマンド)の想定を教えてください。 また「OIDCの仮名」は具体的にどのようなデータになりますでしょうか。		基本設計時に検討とします。
26	質問	4	別紙3.機能一覧表 最低動作アプリバージョン管理	アプリ・OSバージョンチェックAPIを新規作成する想定です。 バックエンドにチェック条件となる各種バージョンを運用で管理し、APIでチェック結果を返却する想定でよろしいでしょうか。		モバイルアプリから API リクエスト時に HTTP ヘッダに OS / バージョンをカスタムヘッダとして付与して判定する形を想定しています。 バックエンドアプリケーションでは、フィルタなどの処理によって本処理の前に最低動作アプリケーションを満たさない場合は指定のエラーを返却する形とします。

「令和5年度 個人向け認証アプリケーションの開発」調達仕様書に対する意見・質問について

連番	意見内容					デジタル庁回答
	質問／意見	頁	項目名	意見・質問等	理由（意見の場合のみ記述）	
27	質問	4	別紙3.機能一覧表 利用規約・プライバシーポリシーの再同意誘導機能	利用規約・プライバシーポリシー取得APIを新規作成する想定です。 バックエンドに最新の利用規約・プライバシーポリシーに関する情報を運用で管理し、APIでは特別な加工なく返却する想定でよろしいでしょうか？ スマホアプリが利用者の同意済みのバージョンを保持し、APIから返却されたバージョンとの差異を判定する想定です。		他端末を考慮し同意済みバージョンはバックエンドで管理してください。 APIでの返却データに関しては、基本設計時に検討とします。
28	質問	4	別紙3.機能一覧表 サーキットブレーカー機能	OCSP失効確認エラーの場合、数回のリトライ後にCRL失効確認に切り替えるなどの方式はご要件に当てはまりますでしょうか。 もしくはNW遮断などインフラで対応する方式を想定されていますでしょうか。		基本設計時に検討とします。
29	質問	4	別紙3.機能一覧表 オンボーディング機能	オンボーディング用データ取得APIを新規作成する想定です。 バックエンドにオンボーディング情報(詳細未定)を運用で管理し、APIでは特別な加工なく返却する想定でよろしいでしょうか。		基本的に特殊な加工は不要の認識ですが、内部のデータは UX の改善を継続的に行うために低コストで変更可能な仕組みを想定しています。
30	質問	4	別紙3.機能一覧表 連携対象RP一覧機能	RP一覧APIを新規作成する想定です。 バックエンドにRP情報(詳細未定)を運用で管理し、APIでは特別な加工なく返却する想定でよろしいでしょうか。 RPに関する情報取得として、フローp18「呼び出し元情報取得」もAPI提供が必要でしょうか(ClientIDを指定したRP情報取得)		少なくとも利用者の各RPへの認可有無を含む必要があります。詳細に関しては基本設計時に検討とします。
31	質問	4	別紙3.機能一覧表 お問い合わせ機能	問い合わせ先情報提供APIを新規作成する想定です。 バックエンドに問い合わせ先情報(詳細未定)を運用で管理し、APIでは特別な加工なく返却する想定でよろしいでしょうか。		基本設計時に検討とします。
32	質問	4	別紙3.機能一覧表 お知らせ表示機能	お知らせ情報提供APIを新規作成する想定です。 バックエンドにお知らせ情報(詳細未定)を運用で管理し、APIでは特別な加工なく返却する想定でよろしいでしょうか。		基本設計時に検討とします。

「令和5年度 個人向け認証アプリケーションの開発」調達仕様書に対する意見・質問について

連番	意見内容					デジタル庁回答
	質問／意見	頁	項目名	意見・質問等	理由（意見の場合のみ記述）	
33	質問	5	別紙3.機能一覧表 分析ログ受信機能	「分析ログ受信機能」にて受信するログは、別紙3 個人認証サービス・クライアントアプリケーションのうち、エラー発生情報、テレメトリー情報が該当する認識で合っていますでしょうか。 またそれ以外のログがあれば、ご教授願いたい。		基本設計時に検討とします。
34	質問	7	別紙5.非機能要件一覧表 可用性要件	「大規模システム変更に伴うサービス全体の計画停止は、デジタル庁及び関連RPとの協議の上で行うこと」とありますが、関連RPとの「協議」の主体者は貴庁、受託者のいずれになりますでしょうか。		受託者ではなくデジタル庁等が主体者となります。
35	意見	8	別紙3.機能一覧表 独自スコープ	「独自スコープ」を追加するとありますが、独自のスコープを追加した場合、RP側で使用しているOIDCと差分が発生するため、RP側への影響が懸念されます。	独自クレームを使用していたため、RP側での対応が複雑になったケースがあります。	基本的な情報は OIDC の仕様に則り、拡張部分を独自に定義する想定です。 また、典型的な属性情報以外に、将来的に API に対する認可も提供する想定となるため必要である認識です。
36	意見	8	別紙5.非機能要件一覧表 耐障害性	「クラウドサービスの利用により可用性を含めたSLA/SLO/SLIを定義し、冗長性を担保する」とありますが、クラウドサービスにて提示されているSLA/SLO/SLIにてご要望は充足されるという理解で合っていますでしょうか。 また運用面等を考慮した総合的なSLAを要望される場合は、体制及び費用等に影響するため、具体的な目標値を示していただきたい。		本調達時点ではクラウドサービスにて提示されているSLA/SLO/SLI で要件を満たしています。 具体的な目標値は記載している認識ですのでそちらもご確認ください。
37	質問	9	別紙5.非機能要件一覧表 目標復旧水準（業務停止時）	「DRサイトへの切り替え」とありますが、DR先は国内サイト限定となりますでしょうか。 （AWSの大阪リージョンでは一部制約があるようです）		本システムの性質上、国内サイト限定とします。 リージョン間での機能差分に関しては、問題が発生した際に都度協議させてください。
38	意見	12	別紙5.非機能要件一覧表 オンラインレスポンス	「mTLS 認証」「外部API（JPKI連携）」のレスポンスは、ネットワーク、システム、デバイス等の他責要因による影響があるため、レスポンスの測定／指標設定区間は自責範囲に限定していただきたい。	レスポンスは、ネットワーク、システム、デバイス等、他責要因による影響があるため。	mTLS 認証に関しては自責範囲の認識です。 一方、外部APIに関しては一定の考慮をしますが、考慮する際の指標の算出方法などに関しては、詳細は基本設計時に協議させてください。
39	質問	14	別紙3 機能一覧表 ログ表示機能	CloudWatchのメトリクスやアラームなどをカスタマイズする対応はご要件に叶いますでしょうか。		ログ・メトリクスに対するクエリやダッシュボードはカスタマイズが必要になる認識ですが、基本的には CloudWatch で満たせます。
40	質問	14	別紙3 機能一覧表 Direct Connect	JPKIシステム側が専用線接続の接続点を準備しており、そちらとDirectConnect経由で接続するという理解で合っていますでしょうか。		個人認証サービス側の要件定義に合わせて接続します。JPKI側は、専用線でもインターネット越しでも接続可能と認識しています。専用線にて AWS DirectConnectを利用するかは、コスト計算等も必要になると認識しているので現時点では決めずに Network設計時に決定することしたいと思います。
41	意見	15	別紙3 機能一覧表.pdf 分析ログ	ログ出力はCloudWatchLogs経由で環境内のS3に出力することを想定します。その場合、 CloudWatch、S3を参照するアクセス権をご提供する方法もございます。	2重投資と捉えられる場合もあるため。	想定頂いているとおりです。
42	意見	27	別紙5.非機能要件一覧表 伝送データの暗号化	「本システムでは処方・調剤に係る情報などを扱うため重要情報の暗号化が必須である」は不要と思われます。	本案件には関係しない内容のため。	御指摘の通りですので、削除します。
43	意見	31	別紙5.非機能要件一覧表 セキュリティ要件	「以下に示すなりすまし、改ざん、否認の防止対策を講じること」とありますが、「以下」の内容がありません。	例の欠落と思われます。	御指摘の通りですので、(以下に示す)を削除します。
44	質問	P35、P36	別紙5.非機能要件一覧表 5．移行性要件	P35、P36の5．移行性要件について、一部内容は異なりますがページ重複していると思われます。 いずれのページを正として良いでしょうか？		P35を削除して P.36⇒ P.35とします。
45	意見	42	別紙5.非機能要件一覧表 7．テスト要件 3総合テスト実施方針案	右上注釈 「※下記は想定であり、実際の内容は支払基金と協議の上、決定すること」については、誤記と思われます。	誤記と思われます。	ご指摘の通りですので修正いたします。
46	意見	43	別紙5.非機能要件一覧表 4　総合テスト実施方針案	「スマホへ Google Play, Apple Storeからアプリケーションをダウンロードする際に JPKI対象機種のスマホか非対象の機種かのテストを行い、JPKI対象機種のみがダウンロードできるかの運用テストを実施する」とありますが、Apple App Storeの誤記と思われます。	誤記と思われます。	ご指摘の通りですので修正いたします。
42	質問	調達仕様書 p.5	1(4) 業務・情報システムの概要	R4年度は現行GBizID運用保守事業者様にて一部機能を構築していると理解していますが、どこまで構築されているか、ご教示ください。		OAuthのフローの実装＋署名用の機能を構築しております。入札公告時に基本設計書を閲覧できるよう情報提供する予定です。

「令和5年度 個人向け認証アプリケーションの開発」調達仕様書に対する意見・質問について

連番	意見内容					デジタル庁回答
	質問／意見	頁	項目名	意見・質問等	理由（意見の場合のみ記述）	
43	質問	調達仕様書 p.5	1(4) 業務・情報システムの概要	スマホJPKI対応（スマホ搭載の証明書を利用した認証、電子署名）は本調達のスコープに含まれるのでしょうか。（券面入力補助APを使用した基本4情報の読取りに影響あり）		スマホJPKIは本調達の範囲外とします。本調達開発中に対応する場合は、デジタル庁内のモバイルアプリ開発チームにて対応します。
44	質問	調達仕様書 p.5	1(4) 業務・情報システムの概要	図の中で、バックエンドに「統計・分析機能」がありますが、本機能は別紙3_機能一覧表上のどの機能に該当しますでしょうか。 （図に記載されているシステム以外との連携有無が発生する想定かどうかを確認させていただきたい意図になります）		別紙3機能一覧表→機能一覧表（管理ツール）→統計情報表示機能です。
45	質問	調達仕様書 p.5	1(4) 業務・情報システムの概要	個人認証サービス・運営主体端末と、今回構築する個人認証サービス（バックエンド）との基盤接続作業については、本調達のスコープ外という理解で合っていますでしょうか。		ご理解のとおりです。
46	質問	調達仕様書 p.6	1(7) 作業スケジュール	個人認証アプリはR5年5月からユーザビリティテスト・アクセシビリティテストとなっていますが、この時点までに初期開発された個人認証アプリはできている理解であっていますでしょうか。		ご理解のとおりです。
47	質問	調達仕様書	2(1)調達範囲	なお、本調達範囲には運用設計、RP 移行支援 は含まれない。 →運用設計を実施する時期・担当事業者について現時点の想定があれば、ご教示ください。		現時点で決まっておりません。
48	質問	調達仕様書 p.9	3(1) 個人認証サー ビススマホア プリ（モバイルアプリケーション テスト ・デザイン 支援 業務	個人認証サー ビススマホア プリ（モバイルアプリケーションのアプリストアの審査等の本番リリースに係る諸手続きは、本調達のスコープに含まれるでしょうか。		デジタル庁で実施する想定です。
49	質問	調達仕様書	3(2)バックエンド開発業務	受注者が構築する開発環境、接続検証環境、本番環境はガバメントクラウド上に構築する理解で合っているでしょうか。		ご理解のとおりです。 ※なおバックエンドで完結する開発作業環境はガバメントクラウドの範囲外のため除外
50	質問	調達仕様書	3(2)バックエンド開発業務	開発したコード等は当庁が指定する構成管理ツール内に登録し、最新情報を管理する →構成管理ツールとして何を利用するか、現時点の想定があればご教示ください。		デジタル庁にて契約済のGithubを想定しています。
51	質問	調達仕様書	3(2)バックエンド開発業務	公開用のAPI リファレンスのページ →別調達の「APIカタログサイト構築」の検討結果も影響すると想定されますが、どのように連携するか現時点の想定があればご教示ください。		APIリファレンスページは調達範囲外とします。
52	質問	調達仕様書 p.14	3(4)現行事業者からの引継ぎ（引継受け）について	GビズIDの基盤保守運用業務一式変更案件で別途開発するサービスの引き継ぎ時期は、いつ頃を想定されているでしょうか。		GビズIDにて開発中のものは、成果物のみを契約時点で引き渡す形を想定しております。 対象システムは既存ベンダーが運用を行い、保守運用業務の引き継ぎは発生いたしません。 ※対象システムの本番リリースは七月を想定するため、本案件開始後の変更は都度共有予定
53	意見	調達仕様書 p.14	3(5)成果物	個人認証サービススマホアプリ（モバイルアプリケーション）におけるユーザビリティテストの対象者は、一般の方（ITリテラシー、年代などいくつかの観点で層を分類）を想定されていますでしょうか。 その場合は、仕様書にその旨の追記のご検討をお願い致します。		デジタル庁で設定しているペルソナがあり、そちらに従って一般の方を集めてテストをすることを想定しております。
54	意見	調達仕様書	6(4)複数事業者による共同入札	以下の文言を追記いただきたくご検討をお願いいたします。 「共同入札を行う複数の事業者は、事業者間において締結する協定で本調達にかかる業務の分担を定めた場合、自己が分担する業務の遂行に関してのみ、デジタル庁に対し責任を負うものとする。」 ※本項について、過去の調達「01 調達仕様書【口座付番 公金受取口座Ph3】」と同様の文言にしていただきたいと考えます。		追記致します
55	質問	別紙2_想定する開発体制案及び必要ツール一覧.pdf p.2	モバイルアプリテスト支援 iOSアプリエンジニア・Androidアプリエンジニア	iOS・Android共に、スキルセットの幅が広く、対象とするモバイルアプリの開発作業のほぼすべての領域をカバーできるエンジニアのように読めるが、テストチームの人員として全て必須のスキルなのか？それともNTHでも構わない部分があるか？（SwiftUI/JetpackComposeによるUI開発を含むネイティブアプリ開発、アクセシビリティの知見、CI/CDの構築、MNC読み取りに必要となる技術要素の知識・経験、など全てをカバーするとなると、全領域の開発作業を担当できるレベルのハイスキルなエンジニアが求められているように読める）		モバイルアプリケーション開発は調達範囲外とします。
56	質問	別紙2_想定する開発体制案及び必要ツール一覧.pdf p.2	バックエンド開発 フロントエンドエンジニア	「React/Next.js を用いたフロントエンドフレームワークでの開発経験」とあるが、これは運用管理画面開発のフレームワークを指していて、React/Next.js の利用が必須であるということか？それとも協議の上、他のフレームワークを選定することも可能か？		協議の上で他のフレームワークを選定することも可能です。スキルセットとして同等の設計・開発能力を期待します。
57	質問	別紙3 p.4		PUSH通知は本サービスから直接クラウドサービスに連携して送る理解でしょうか。（開示Sでも同様の仕組みを保持しているが、別の仕組みとして構築するか）		別の仕組みとして構築します。
58	質問	別紙3 p.7	OIDC	クライアント認証方式では、「以下の認証方式をサポートすること」に「client_secret_post」が含まれている。 →FAPI Part1では「client_secret_post」が利用できない仕様ですが、認証方式として含める想定でしょうか。 FAPI Part1記載箇所：https://openid.net/specs/openid-financial-api-part-1-1_0-final.html#authorization-server		RP側の事情が発生することを考慮し、含める想定とします。 ※ライブラリ・SaaSなどを使った場合含むコストはない認識
59	質問	別紙3 機能一覧表 p.3	個人認証サービス アプリ連携共通機能 DeepLink 対応	UniversalLinks(iOS)や、AppLinks(Android)に対応する場合、URLとアプリを紐付けるためにJSONファイルのホスティングが必要になるが、Firebaes DynamicLinksなどmBaaSの機能を利用する想定か？それとも自前でホスティングする想定か？ また、ホスティングに関する作業は、モバイルアプリ開発作業に含まれているか？それともバックエンド側作業に含まれる想定か？		現時点では自前でホスティングする想定ですが、要件上必要になる場合は検討します。ホスティングに関わる作業はバックエンド開発作業に含みます。 ※ファイル内容はデジタル庁側開発担当者と協議の上で決定
60	質問	別紙3 機能一覧表 p.4	初期登録機能 利用規約・プライバシー ポリシー機能	利用規約・プライバシー ポリシー機能は、モバイルアプリとは別に提供する想定に見えるが、提供するコンテンツについては、バックエンド側の作業という想定か？ それともモバイルアプリ開発側から提供されるものか？		コンテンツ管理は改訂や更新を鑑みてバックエンド側で保持・提供します。 表示をアプリにて行うかWebView等で行うかは要件定義時に協議の上決定します。
61	質問	別紙3 機能一覧表 p.12	利用状況の収集	収集した利用状況のデータを利用して、運用管理のダッシュボード等に表示するような機能は想定しているか？Firebase Crashlytics/Analitics等外部サービスのコンソールまたは提供されているAPIで取り扱えればよいか？		ISMAPを満たすSaaSの利用を想定しています。

「令和5年度 個人向け認証アプリケーションの開発」調達仕様書に対する意見・質問について

連番	意見内容					デジタル庁回答
	質問／意見	頁	項目名	意見・質問等	理由（意見の場合のみ記述）	
62	質問	別紙3 機能一覧表 p.12	サービス状況表示機能 必須アップデート通知	「APIリクエスト[にバージョンを付けて」とあるが、API側の複数バージョンを並行稼動させるような要件はあるか？		後方互換性が完全に無いバージョン以外は、同一アプリケーション内でパスベースで分離(ex. /v1/xxx, /v2/xxx)をした上で新旧バージョンの並行稼働を想定しています。 検証コストの削減などを目的とし、一定バージョンごとに強制アップデートをすることを検討しております。
63	質問	別紙3 機能一覧表 p.14	個人認証サービス 運用管理システム 運用管理	ダッシュボード機能は、バックエンド側のログをベースに状況把握できるようにする目的のものか？ スマホアプリ側のテレメトリーも見れる必要があるか？（例えば、Firebase Analyticsで取得するアプリログをBigQueryにexportして、そのログを元にした情報をダッシュボードに表示する、など）		ご認識のとおりです。
64	質問	別紙4-1 p.1		本案件の対象はID連携のみであり、属性連携（＝個人認証サービスで管理する属性情報をRPに連携する）は対象外の認識で合っているでしょうか。		券面事項入力補助APで取得する情報および、利用者証明用電子証明書のシリアル番号以外の属性情報は、本調達の範囲外とします。 しかしながら、RPに対して関連システムがデータ操作をAPIで公開するための認可機構のベースは本調達範囲内で実現します。 ※Token Introspection等
65	質問	別紙4-1 p.1		今回構築する個人認証サービスにおいて、RPへの課金は実施される想定でしょうか。		現時点で課金は想定しておりません。
66	質問	別紙4-1 p.1		【念の為確認】本サービスにおいて、利用者用電子証明書の失効確認はCRL、署名用電子証明書の失効確認はOCSPを利用する理解でよいでしょうか。		ご理解のとおりです。
67	質問	別紙4-1 p.7		端末内に基本4情報を保持する用途について、ご教示ください。※端末内に基本4情報を保管する場合、変更時の運用を考える必要があると考えます。		検討中です。
68	意見	別紙4-1 p.10		旧シリアルと新シリアルの付け替えを行っているが、シリアル履歴を管理するテーブルを作成する必要があると考えます。 現在開示で次のユースケースで利用しており、今後RP側でも利用すると想定しています。 ・API基盤への自己情報/お知らせの送信履歴の取得 ・API基盤からの自己情報取得要求が旧シリアル→新シリアル変換		ご指摘の通りのため機能一覧に追加いたします。
69	質問	別紙4-1 p.10		フロー上「券面入力補助AP」と「利用者用電子証明書」のカード読取りを1回にまとめて実施するように認識しましたが、制度的/技術的に可能なのでしょうか。		都度認証するか／省略可能とするかはRP側で選択できるようにする想定です。
70	質問	別紙4-1 p.16		「前回認証時の権限があり、かつ認可済みRPの場合はマイナンバーカードを用いた認証を省略する」 →都度マイナンバーカードによる認証を実施しなくて問題ないのでしょうか。		検討中です。
71	質問	別紙4-1 p.12	OIDC	「クライアント権限アクセストークン」と「ユーザ権限アクセストークン」の違いについてご教示ください。		クライアント権限アクセストークンは Phase1 での基本設計時に要件から落としたので、本調達からも外します。
72	質問	別紙4-1 p.14	OIDC	p.14「㉕ユーザ認証リクエスト」は認可コードを発行しないフロー、p.28「㊻認可同意リクエスト」は認可コードを発行するフローを利用する認識で合っているでしょうか。		ご認識のとおりです。
73	質問	別紙4-1 p.9、19	OIDC	p.9「OAuth 認可サーバー」と、p.19「IdP(OP)サーバー」の違いについてご教示ください。		表記揺れで同一のものを想定しております。
74	質問	別紙4-2 p.91		「券面事項入力補助AP で基本4情報読取り＋署名用証明書読取り +UUID 送信」 →マイナンバーカードの読取り1回で実現可能なものでしょうか。		読み取り自体は二回行うが、かざし行為を一回で行う形を想定しております。
75	質問	別紙5 非機能要件 p.4		「本システムは基本的にクラウド内で完結する仕組みとし、本サービスシステムの安全かつ完全な形での流通を実現すること。」 →シリアル番号については、クラウド環境の管理のみでOKでしょうか。		全てクラウド上を想定しておりましたが、協議のうえ決定します。
76	意見	別紙5 非機能要件 p.9		「本サービスにおける稼働率の目標は、99.9%とする。」 →個人認証サービスを利用するRPの可用性に照らして問題ないか、確認が必要と考えます。		これ以上の可用性を求める RP の検討が始まってから検討します。 ※スリーナイン以上を求めるとコストが跳ね上がるため
77	質問	別紙5 非機能要件 p.9		「なお、バックアップはリージョン間で相互に保管すること。」 →本案件では、マルチリージョンによるホットスタンバイ構成とする想定でしょうか、またはバックアップデータのみの保管とする想定でしょうか。		バックアップデータのみの保管を想定しております。
78	質問	別紙5 非機能要件 p.38		「未成年・成年被後見人・海外からの渡航者などに関しても考慮すること。」 →代理人による利用は本案件のスコープ外と認識しておりますが、合っているでしょうか。		代理人はスコープ外で齟齬ありません。一方、未成年・成年後被後見人は利用者証明のみは可能なのでスコープ内とします。
79	質問	別紙5_非機能要件一覧表 p.33~35		サービスイン時の本番切替に係る移行計画や準備・作業実施のスケジュールが、調達仕様書の作業スケジュールに記載されておりませんが、作業遂行上考慮しておくべきマイルストーンや制約等があればご教示ください。		移行は当調達では行いません。よって移行リハーサルなども発生しませんので、仕様書を更新します。
80	質問	別紙5_非機能要件一覧表.pdf p.38	システム環境要件	モバイルアプリの動作対象OSバージョンや動作対象機種はマイナポータルアプリと同様と捉えればよいか？		モバイルアプリテスト支援は、当調達範囲外とします。
81	質問	別紙5_非機能要件一覧表.pdf p.40	テスト要件	計画したテストの実施に必要となる機材（スマートフォン）の調達は誰が行うか？支援業務担当が用意する想定？		モバイルアプリテスト支援は、当調達範囲外とします。
82	質問	別紙5_非機能要件一覧表.pdf p.40	テスト要件	多機種テストは、別途「受入テスト」の段階でQuality Assurance事業者が実施する想定でよいか？		モバイルアプリテスト支援は、当調達範囲外とします。
83	質問	（4）業務・情報システムの概要		個人認証サービス・運営主体端末は調達範囲外との認識でよろしいでしょうか。 この場合、閉域接続用のNW回線（インターネットVPNを想定）、AWS VPNの設定も本調達の範囲外との認識でよろしいでしょうか。		個人認証サービス・運営主体端末は調達範囲外、接続部分は調達範囲です。

「令和5年度 個人向け認証アプリケーションの開発」調達仕様書に対する意見・質問について

連番	意見内容					デジタル庁回答
	質問／意見	頁	項目名	意見・質問等	理由（意見の場合のみ記述）	
84	質問	（4）業務・情報システムの概要		個人認証サービス・運営主体端末を利用する際の認証・セキュリティ関連の設定についても本調達の範囲外との認識でよろしいでしょうか。		本調達範囲外です。
85	質問	（4）業務・情報システムの概要		赤枠で囲われている今回の調達範囲である以下の主要機能と別紙3機能一覧表の機能との対応表はございますでしょうか。 ・個人認証サービススマホアプリ ・【個人認証サービス】 「アカウント認証機能／ID連携機能（OIDC OP）／デバイス間ID連携機能／アカウント情報管理機能／RP管理機能／Webサーバ機能」 「WebAPIアプリ用機能／WebAPI認証認可機能／WebAPI電子署名機能／WebAPI管理用API」 「運用管理ダッシュボード機能／ログ管理機能／監査証跡管理機能／統計・分析機能」 「OCSP連携機能／失効情報取得機能」		ございません
86	質問	（4）業務・情報システムの概要 機能一覧表		#4のご回答を受けて追加で4点確認させてください。 弊社側で、今回の調達範囲である主要機能（赤枠部分）と別紙3機能一覧表の機能との対応付けを実施した結果、主要機能（赤枠部分）の「Webサーバ機能」「WebAPI電子署名機能」「WebAPI管理用API」に対応する機能は無く「統計・分析機能」に対応する機能は1つという結果になりました。 ・「Webサーバ機能」は、デバイス間ID連携機能に関する画面を指す認識で相違ありませんでしょうか。		相違ありません。
87	質問			・「WebAPI電子署名機能」は、機能一覧のバックエンド側に電子署名機能がないと思われますが、GビズIDから引き継ぐ想定の機能のため記載がない理解でよろしいでしょうか。		認識の通り齟齬ありません。
88	質問			・「WebAPI管理用API」は、機能一覧のどの機能が該当しますでしょうか、また具体的にどのような機能になりますでしょうか。		機能一覧内の運用管理タブの各種機能を想定しています。大半は AWS 上のマネージドサービスで実現可能な認識ですが、提案時の構成で一部独自に開発する必要がある場合は本カテゴリにて管理してください。
89	質問			・「統計・分析機能」は、個人認証サービス管理ツールの#7統計情報表示機能をさすと考えておりますが、認識相違ありませんでしょうか。また、本機能はダッシュボード機能とは別に独自に統計・分析する機能を開発する想定でしょうか。		その想定です。
90	質問	（1）調達範囲		運用設計は本調達の範囲外との記載がございますが、システムの起動・停止、アプリケーションのSI等のオペレーションに関する運用設計は範囲に含まれる認識でよろしいでしょうか。(P13～14に記載の「個人向け認証アプリケーションの保守運用（仮）受注者への引継ぎ」項目に「オペレーション業務手順」が含まれるため。)		運用設計は本調達の範囲外です。
91	質問	個人認証サービス 運用管理システム 項番8 ヘルプデスク機能		#6のご回答を受けて追加で1点確認させてください。 「RP側のヘルプデスクとの連携を考慮した運用設計とすること」について、運用設計は本調達の範囲外になるが、オペレーション業務手順は範囲に含まれる、という理解でよろしいでしょうか。		認識に齟齬はないですが、ヘルプデスクとの連携を視野に入れた設計（ヘルプデスクでの対応に必要なデータ・ログ保管や、参照するための仕組みの検討）を行なっていただくことは本調達の範囲内になります。
92	質問	3．作業の実施内容		準委任部分の作業ボリュームについて想定以上の工数が必要となった場合は、デジタル庁様にて吸収される想定でしょうか。（事業者の生産性が想定通りである前提で） ※急な体制増強があった場合にスキルマッチした要員を確保できるかの観点での確認です。		ご認識のとおりです。
93	質問	3．作業の実施内容		・開発作業等はモバイルアプリ（デジ庁支援）部分に関しても基本リモート作業と考えてよいでしょうか。 ※開発場所がデジタル庁に指定されることはございますでしょうか。		ご認識のとおりです。
94	質問	3．作業の実施内容		「開発により実現する機能は、受注者により提案後、当庁と協議し決定する」とございます。これは機能一覧表に明記されたもの以外に事業者の追加提案により実現する機能があった場合は協議の上、決定するという理解で正しいでしょうか。 ※追加機能の実現を想定した場合、提案時にお見積金額に影響すると考えたための確認です。		追加はない想定だが多少の変更はあるかもしれないことを見込んだ記載です。
95	質問	（2）バックエンド開発業務		各環境ともGov-Cloudではないクラウドサービスプロバイダーを使用するという認識でよろしいでしょうか。		ガバメントクラウドを使います。
96	質問	＜モバイルアプリケーション及びバックエンド開発共通参考情報＞		「事業者の申請に係るUX/UI」とはGビズIDの利用のことを想定されている認識で正しいでしょうか。 また、「利用者を想定したユーザエクスペリエンス（UX）及びUIを実現していくための基準」というのはデジタル庁様にて開発をするモバイルアプリのUI/UXの基準を事業者側で作成するというイメージでしょうか。		ご認識のとおりです。
97	質問	公開用の API リファレンスのページ		インターネット上に公開するWebページとして作成する認識でよろしいでしょうか。また言語は日本語と英語両方に対応する認識でよろしいでしょうか。 ※今回構築するシステム上で公開するものを作成するのか、単にHTMLとして作成するのかという確認です。		APIリファレンスページは調達範囲外とします。
98	質問	3．作業の実施内容		継続事業者等への引継ぎについて、回線や機器保守についても記載があります。これは当該事業の受託事業者が準備したものを後続事業者が準備できるような情報の整理という理解で正しいでしょうか。		ご認識のとおりです。
99	質問	開発体制 想定するスキルセット		バックエンド開発において、開発体制と想定するスキルセットとの対応表はございますでしょうか。		想定するスキルは別紙2にありますが、体制との紐付けは行っておりません。バックエンド開発は請負ですので細かな指定はしておりません。

「令和5年度 個人向け認証アプリケーションの開発」調達仕様書に対する意見・質問について

連番	意見内容					デジタル庁回答
	質問／意見	頁	項目名	意見・質問等	理由（意見の場合のみ記述）	
100	質問	想定するスキルセット バックエンド開発 フロントエンジニア		バックエンド開発のフロントエンド部分は別紙4の画面遷移図よりデバイス間連携関連の画面(※)が対象と想定しております。本画面を「TypeScript」や「React/Next.js」を用いて開発するという理解であっておりますでしょうか。 (※)デバイス間連携関連の画面 デバイス間連携開始画面 デバイス間連携確認コード画面 デバイス間連携待機画面 デバイス間連携画面		Next.js までは必要とならない可能性は高いですが、スキルとして最低限これらのものを正しく設計できる人員を配置していただきたいです。 同一画面内で動的な振る舞いが要求されるため、フロントエンドアプリケーションの実装が必要となる認識です。
101	質問	個人認証サービス IdP(OP)システム 項番1 利用者証明用電子証明書を用いた、mTLSクライアント認証機		mTLSによるクライアント認証ということで、RFC 8705に規定されている、tls_client_authを実施したいという理解で正しいでしょうか。また、その際に利用するクライアント証明書は、マイナンバーカードの利用者証明書であるという認識でよろしいでしょうか。		mTLS はあくまでも利用者認証に用いるだけを想定しているため、tls_client_auth まではスコープとして含めていません。 認証に用いるクライアント証明書は、マイナンバーカードの利用者証明用電子証明書となります。
102	質問	個人認証サービス IdP(OP)システム 項番42 個人認証サービスアプリ利用者向けマニュアル・FAQ機能		想定している管理ツールやCMS等はございますでしょうか。		現時点ではないので提案していただけますと幸いです。広く使われているツールであることが望ましいです。
103	質問	個人認証サービス 運用管理システム		「調達仕様書_令和5年度個人認証アプリ開発支援.pdf」P.6の図ではJPKIとインターネット経由で接続する構成となっていますがどちらが正しいでしょうか。		JPKI側の仕様に基づいて決定します
104	質問	業務フロー図		別紙4、P.13ではユーザ認証リクエスト受信後に「㉖利用者証明用電子証明書検証及びユーザ識別」が記載されていますが、P.64には記載されておりません。 記載を省略しており、P.13とP.64のユーザ認証リクエスト受信後の処理は同じである(個人認証サービスアプリから同じWeb APIが呼び出される)という理解でよろしいでしょうか。 ※BPMN図で、P.10の認証処理が「認証サーバー」、P.60の認証処理が「IdP(OP)サーバー」に記載されていることから、念のための確認です。		図表の記載ミスのため修正致します。
105	質問	業務フロー図		Phase1.0の業務フローであるため、本業務に関する機能はすべて実装済みとの理解でよろしいでしょうか。		ご認識のとおりです。
106	質問	（1）知的財産権の帰属		「(1)知的財産権の帰属」の定めにかかわらず、オープンソースソフトウェア所定のライセンスの条件に従って取り扱う認識でよろしいでしょうか。		ご認識のとおりです。
107	質問	(2) 契約不適合責任に関する事項		民法では、「履行の追完」の方法として、「目的物の修補」「代替物の引渡し」「不足分の引渡し」の3つが定められていますが、仕様書に記載の「修補又は履行の追完」という条件は、どの方法を指したものでしょうか。P22(ケ,コ)に受託者から提示しデジタル庁様の了承を得ると記載があり、受託者側で検討できるものと考えてよろしいでしょうか。		ご認識の通り、「履行の追完」の方法として、「目的物の修補」「代替物の引渡し」「不足分の引渡し」の3つがあり、公告の際添付される予定の契約書（案）にも同様の記載があります。 ただし、契約書（案）でも調達仕様書でも、どの方法かは指定はしておらず、最適な方法を選択する形となります。 追完を行う場合は、受託者様から不適合の原因と追完の方法、追完を行った場合の影響についてご提示を頂いた上で、デジタル庁側で方法について判断することとなります。
108	質問	個人認証サービスアプリ サービス状況表示機能 サービス終了時の表示		「サーバー側でコントロールできることが望ましい。」について、サーバ側の機能一覧に記載がないと思われますが、Ph1.0で実装済みのため記載がない、という理解でよろしいでしょうか。		ご認識のとおりです。
109	質問	個人認証サービス 運用管理システム 項番8 ヘルプデスク機能		#6の質問において「運用設計は本調達の範囲外」とご回答いただきましたが、対象箇所の文中に「RP側のヘルプデスクとの連携を考慮した運用設計とすること」と記載がございます。運用設計については、本調達の範囲外という認識で相違ないでしょうか。		運用設計は本調達の範囲外です。
110	質問	Web API システム 項番4 ハッシュ値の暗号化（署名値生成）		クライアントAPIではなくWebAPIを実装するという理解でよろしいでしょうか。		APIは調達範囲外とします。
111	質問	Web API システム 項番7 ハッシュ値の暗号化（署名値生成）		クライアントAPIではなくWebAPIを実装するという理解でよろしいでしょうか。		APIは調達範囲外とします。
112	意見	調達仕様書 P21	(2) 契約不適合責任に関する事項 キ　前項の規定により種類又は品質に関する契約不適合に関し～	契約不適合責任の存続期間について、例えば「成果物の引き渡し後1年間」等、期限を設けることができないか、ご検討いただきたい。	履行を追完するために長期間の体制維持や引き渡し後の長期かつ未確定要素への対応を見込む必要があり、応札業者が限定される可能性や応札金額への影響が大きいと考えるため	責任期間を具体的に定めることはいたしかねます。