別紙１　技術検証項目一覧

項番	分類	項目	内容	デジタル庁	関係事業者	本業務の請負者	設計工程前に着手が必要な項目(要件検討結果報告書に記載が必要)	設計工程以降に完了予定の項目
1-1	mdoc	システム構成の検討	・ mdocを搭載するために必要となるシステムについて、全体構成を作成、検討する。 ・システムの構成要素の開発主体、関係事業者との役割分担、責任分界点を検討する。	○		○	○	
1-2		業務の洗い出し	・mdocに関する業務を検討し、洗い出しを行う。	△		○	○	
1-3		業務フローの検証	・mdocをスマートフォンに搭載する場合に発生する一連の業務フローを作成、検証する。	△		○	○	
1-4		アプリ・システム間のインタフェース検討	・サードパーティーの行政・民間のアプリやシステムがmdocを利用してサービスを提供する場合のインタフェースを検討する。	△	○	△	アプリ設計には必要	
1-5		選択的属性開示の実現性検討	・mdocにおける選択的属性開示を実現するため、必要となる要件（mdoc格納データの生成等を想定）や実装方法を検討する。	○	○	○	○	
1-6		mdoc検証のテスト方法に関する検討	・mdoc利用時のverifierが実施するmdoc検証のテスト方法を検討する。	△	△	○	○	
1-7		各システムとのインタフェース検討	・構築対象のシステムと連携先システムとの接続実現性を検証する。 ・授受するデータの項目、フォーマットの検証を行う。			○	○	
1-8		mdoc profile，格納データ項目・形式の検討 RAのデータベーススキーマの検討	・mdoc profileとして、mdocに格納するDoctype，Namespace，各データの項目を検討する。 ・データ形式をISO/IEC 18013-5/7、ISO/IEC 23220シリーズに準拠するよう変換し、mdocに格納できることを検証する。 ・mdocに格納するデータ項目のうち、ISO/IEC 18013-5/7、ISO/IEC 23220シリーズで規定のない項目の格納方式を検討する。 ・mdoc IACAシステムの RAの データベーススキーマの論理設計を検討する。	△		○	○	
1-9		mdoc ライフサイクル	・マイナンバーカード、スマートフォン、電子証明書、住民情報のライフサイクルを加味した、mdocに関するライフサイクルを検討する。			○	○	
1-10		他サービスとの相互干渉	・同一スマートフォンで本mdocと他のmdocサービスやWalletサービスの両方を利用する場合に相互干渉がないことを検証する。		○	△	アプリ設計には必要	
1-11		利用時の認証方式	・PIN及び生体認証により、本人確認を行った上で、mdocが利用できることを検証する。 ・アクセス権、ユーザビリティについて、検証する。		○	△	アプリ設計には必要	
1-12		暗号アルゴリズムの決定	・mdocで採用する署名の暗号アルゴリズム、鍵長、及びパラメータを検討する。	○		△	○	
1-13		mdocの初期化	・スマートフォン端末の初期化により、mdocを初期化することができるかどうか検証する。		○	△	○	
1-14		mdocパッケージの検証	・mdoc発行システムのパッケージのFit＆Gap分析を行う。			○	○	
1-15		MSO再発行間隔の検討	セキュリティのトレーシング問題を回避するため、MSOを定期的に再発行する間隔を検討する。	△		○		
1-16		HSM Clusterの検討	・AWS Cloud HSM Clusterを利用するか、オンプレミス環境で HSM Clusterを構築するか、IAとの接続性、初期コスト、ランニングコストの観点から考察し検討した上で方式を決定する。	△		○	○	
1-17		DTS機能	米国VICAL相当の DTS機能を 本mdoc IACA Systemでどのように提供するかを検討する。			○		
1-18		mdoc IACAのマルチテナント機能の検討	・mdoc IACAでマルチテナント機能をサポートする場合の要件、実現方式を検討する。またマルチテナント機能が提供できる範囲、提供できない範囲を明確にする。			○		
1-19		プロビジョニング時の本人確認の検討	・署名用電子証明書による電子署名及び顔照合で、厳格な本人確認を行うための方式検討を行う。顔照合は、米国mDLの事例を参考にして検討する。	△		○		
1-20		Reader Authentication Certificateの検討	・mdocを検証する Reader の認証を行うための Certificate の方式、認証局から検証者への配布方法等を含めた運用の検討を行う。またスマートフォンのOSの仕様に合わせた証明書を利用した認証方式の運用を検討する。	△		○		
1-21		最新の利用者情報(4情報）を反映した mdoc再発行の検討	・公的個人認証サービスを利用した最新の利用者情報(4情報)提供サービスを利用して、最新の4情報の mdocを スマホへの PUSH型で発行できる方式、運用を検討する。	△		○		
1-22		スマホ電源オフ時のリトライ処理	プロビジョニング時、スマホ電源オフの要因で、プロビジョニングが失敗した際、スマホ電源オンになったらリトライ処理ができるようにする処理を検討する。また一定期間(例えば1ヶ月)電源オフの状態が続いたらプロビジョニング処理を異常終了する処理を検討する。(異常終了後、スマホ利用者が再度、mdoc発行要求するまで mdocのプロビジョニングは行わない仕様とする。）	△		○		
2-1	UI･UX	既存の行政アプリとの後方互換性	・他の政府機関が提供する認証、署名等に関する行政アプリ（マイナポータルアプリ、個人認証アプリ、利用者クライアント等）との機能の切り分け、統合について検討する。	○		△	○	
2-2		サードパーティアプリにおけるmdoc、電子証明書のユーザビリティ	・サードパーティアプリからmdoc及び電子証明書を利用する際に、ユーザが使いやすい仕組みを検討する。	○		△	アプリ設計には必要	
3-1	悪用防止	不正ルートからのアクセス、OS改造等の防御	・特定の機種に対して、サポート範囲内のOSについて動作検証を行う。 ・OSの機能を調査し、検出可能な不正と実装方針を整理する。 ・実機を用いて、実際に不正な操作を行い検出できるかを確認する。 ・結果をまとめて設計方針として整理する。	○	○	△	○	
3-2		スマートフォン端末のセキュリティ機能を踏まえたセキュリティ対策の検討	・OS側の主要なセキュリティ機能を抽出し、実装上の注意点を調査するとともに、適切なセキュリティ対策を検討する。（具体的な調査の観点として、ホワイトリスト制御、APK署名、業務アプリとの連携等の方式を想定）	○	○	△	○	
4-1	運用	GP-SE新製品、アプレット更新、端末新機種投入時の対応	・GP-SE新製品の投入、アプレット更新及び端末の新機種の投入時に、本システムへの影響の発生する構成要素を抽出する。 ・上記が発生した場合に技術的に評価・検証すべき項目、対応事項を整理する。		○	△		○
4-2		OSバージョンアップ	・OSのバージョンアップ時に想定される課題を抽出する。		○	△		○
5-1	その他	アプリの利用同意/責任分界	・システム全体像に基づき、本システムの利用同意の取得方法や各関係事業者の責任分界検討を行う。	○	○	△	アプリ設計には必要	
5-2		かざし利用の通信性能	・マイナンバーカード対応のICリーダライタ（コンビニ及び保険証で使用されるICリーダライタを含む）とスマートフォンの通信互換性を検証する。	○	○	△		○

凡例
○:実施主体
△:支援