マイナンバーカード機能等のスマートフォンへの搭載に係る実証事業に伴う暗号方式の委託研究

調達仕様書

令和６年４月

デジタル庁

1. 調達案件の概要

1.1. 調達件名

マイナンバーカード機能等のスマートフォンへの搭載に係る実証事業に伴う暗号方式の委託研究

1.2. 調達の背景

デジタル・ガバメント実行計画（令和２年 12 月 25 日閣議決定）において、マイナンバーカードの機能（電子証明書）をスマートフォンに搭載することにより、カードをかざすことなくスマートフォンひとつで様々な手続が可能となり、利用者の利便性が大きく向上するとともに、公的個人認証サービスの利用・普及の促進にもつながるものとされた。

その上で、デジタル社会の形成を図るための関係法律の整備に関する法律（令和３年法律第 37 号）により、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成 14 年法律第 153 号）が改正され、マイナンバーカードの機能（電子証明書）のスマートフォンへの搭載が可能とされた。

デジタル庁では、「スマートフォン用公的個人認証機能管理システム」の構築を行ってきたところ、令和５年５月 11 日より、同システムの運用を開始し、マイナンバーカードの機能（電子証明書）のスマートフォンへの搭載サービスを提供している。

そして、デジタル社会の実現に向けた重点計画（令和５年６月９日閣議決定）において、電子証明書の機能だけでなく、券面入力補助機能など、マイナンバーカードの持つ他の機能についても、優れた UI・UX を実現するため、スマートフォンへの搭載を目指すとされた。この券面入力補助機能なども含めたマイナンバーカードの持つ他の機能をスマートフォンに搭載するために必要なシステムでもあり、各種資格者証の情報を格納できる汎用的なシステムについて、デジタル庁が検討・開発するとともに、スマートフォンに免許情報を記録するモバイル運転免許証における活用を前提に検討を進め、運転免許証とマイナンバーカードとの一体化の運用開始後、極力早期の実現を目指すとされた。

本調達では、利用者の移動端末(スマートフォン)から電子証明書発行機関に送受信される個人情報を含む申請情報等の暗号化通信方式(HPKE 方式)に関する安全性ならびに鍵管理・鍵交換方式の運用面における堅牢性の評価・確認を行うものである。

1.3. 調達目的および期待する効果

デジタル庁が実施するマイナンバーカード機能等のスマートフォンへの搭載に係る実証事業において扱うシステム（以下、「本システム」という。）においては、利用者の移動端末(スマートフォン)から電子証明書発行機関に個人情報を含む申請情報等を送受信する際の暗号化通信方式として、HPKE 方式を採用することを検討している。

本調達では、暗号化通信方式に係る専門的な知見を有する個人（以下、「受託者」という。）に対し、当該の暗号化通信方式（HPKE 方式）に関する安全性評価ならびに鍵管理・鍵交換方式の運用面における堅牢性の評価・確認を行う業務を委託する。

1.4. 業務・情報システムの概要

本調達で取り扱う業務の範囲及び本システムの概要について、以下に示す。

(1) 業務の概要

マイナンバーカード機能等のスマートフォンへの搭載に係る実証事業においては、マイナンバーカードに登録されている個人情報等を含めた項目を基にファイルデータを作成、電子証明書発行機関とスマホとの間で暗号通信を用いて安全にファイルデータを送受信する仕組みを構築している。

ファイル形式を規定するモバイル運転免許証の国際標準である ISO/IEC18013-５及び 18013-７に関するほか、標準化を目指し議論が進められているモバイル身分証の相互運用を目的とした規定群である ISO/IEC23220 シリーズの Part３において、発行時のデータ送受信時に用いる暗号方式に HPKE の End to End Encryption(E２EE)の利用が規定されている。

通信経路の End to End でデータの暗号化・複号化を行う E２EE 暗号化方式に該当する HPKE 暗号化方式における暗号の安全性を担保することが必要である。

本業務では、HPKE 暗号化方式における暗号の安全性評価ならびに鍵管理・鍵交換方式の運用面における堅牢性の評価・確認を行う業務を実施する。

本システムの仕様や本システムにおける HPKE 暗号化方式及び鍵管理、運用に関する詳細な仕様については、関係事業者と受託者との間で秘密保持契約を締結後に開示することとする。

(2) 情報システムの概要

本システムに関する一連の業務（以下、「関連業務」という。）の概要について、以下の「図表 1-1 関連業務の概要」に示す。

図表 1-1 関連業務の概要

項番	業務	業務 （小分類）
1	発行	・ スマホ用電子証明書等の発行を行う。
2	失効	・ スマホ用電子証明書等の失効を行う。
3	更新	・ スマホ用電子証明書等の更新を
4	一時停止	・ スマホ用電子証明書等の一時停止を行う。
5	一時停止解除	・ スマホ用電子証明書等の一時停止解除を行う。
6	自動更新	・ 自動更新を行う。
7	生成	・ ハッシュ値生成等を行う。
8	署名	・ 対象に電子署名を行う。
9	TL・証明書管理	・ TL および TL に追加する証明書などの管理を行う。
10	利用	・ スマートフォンから提示(presentation)、利用を行う。
11	スマホ用電子証明書利用	・ スマートフォンに発行したスマホ用署名用電子証明書およびスマホ用利用者証明用電子証明書のかざし利用を行う。
12	PIN/パスワード初期化	・ スマホ用電子証明書の PIN・パスワードの初期化を行う。
13	電子証明書の情	・ スマホ用電子証明書の有効性を JPKI(OCSP レスポンダ)へ確認する。

	報確認	
14	通知	・ 利用者へ各種通知を行う。
15	運用保守業務	・ スマートフォン用公的個人認証機能管理システム全体の運用保守を行う。

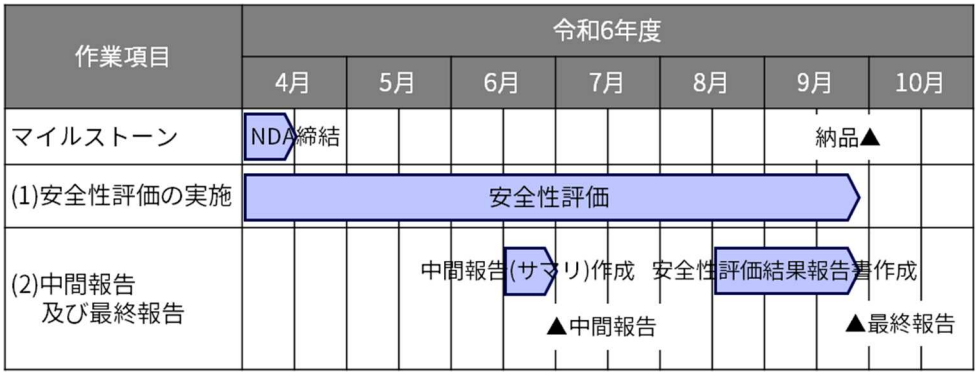
1.5. 契約期間

本業務の契約期間は、契約開始日から令和 6 年 9 月 30 日までとする。

1.6. 作業スケジュール

本業務の作業スケジュール（想定）について、以下に示す。詳細は業務開始後にデジタル庁と協議の上、決定すること。

図表 1-2 本業務の作業スケジュール



1.7. 調達担当課室・連絡先

本調達仕様書に関する問合せ先は以下のとおり。

〒102-0094

東京都千代田区紀尾井町 1-3 東京ガーデンテラス紀尾井町 19 階

デジタル庁 国民向けサービスグループ マイナンバーカード担当

（TEL：03-4477-6775、E-Mail：mynumber_smartphone@digital.go.jp）

2. 調達案件及び関連調達案件の調達単位、調達の方式等に関する事項

2.1. 本調達案件に関連する調達案件

本調達案件に関連する調達案件について、以下に示す。

図表 2-1 関連する調達案件の一覧

項番	調達案件名
1	マイナンバーカード機能等のスマートフォンへの搭載に係る実証事業
2	マイナンバーカード機能等のスマートフォンへの搭載に係る実証事業（SMP 設計・製造）
3	マイナンバーカード機能等のスマートフォンへの搭載に係る実証事業（認証局・発行局の設計構築）

3. 作業の実施内容に関する事項

3.1. 作業の内容

(1) 暗号化方式（HPKE 方式）及び鍵管理等を含めた安全性評価の実施

【作業内容】

1. 暗号プロトコルの評価

   HPKE 方式で利用される複数の暗号プロトコルの組合わせにおいて、サイドチャネル攻撃等のセキュリティの脅威分析を行ない、HPKE 全体として脆弱性の有無等の暗号の安全性評価を実施する。

2. 暗号プリミティブの解析

   暗号プリミティブとは、暗号化、復号化の中心となる基本暗号のことを指す。プリミティブは暗号として利用した場合の安全性の根拠となるアルゴリズムとなり、素因数分解問題、離散対数問題、楕円曲線上の離散対数問題といったものが一般的である。ここでは、HPKE で利用される複数の暗号アルゴリズム（具体的には、DHKEM, NIST P256, SHA256 HKDF, AES256 等）の安全性を評価する。

3. 実際の暗号システムの設計の解析

   実際の HPKE のプログラム実装の鍵管理仕様も考慮して、本システム全体での HPKE 利用の安全性を評価する。本システム全体での実際の運用等を考慮した HPKE の安全性評価を行う。特に HPKE を利用した End to End でのスマホと発行機関間における暗号利用において、End to End ではない中継サーバ等での情報漏洩が発生しないか解析を行なう。

(2) 中間報告及び最終報告

受託者は、本業務の実施状況について、「中間報告書（サマリ）」を作成し、中間報告を行うこと。中間報告の実施時期については、作業着手後 3 カ月頃の提示を想定するが、詳細はデジタル庁と協議の上決定すること。

また、受託者は、「安全性評価結果報告書」を作成し、本業務の完了時に、最終報告を実施すること。

なお、受託者は、納入成果物について事前にデジタル庁のレビュー及び承認を得た上で、納期までに納品すること。

3.2. 納入成果物の範囲、納品期日等

(1) 納入成果物

受託者は、下表に示す納入成果物について、納入期限までに納入すること。なお、納期については、必要に応じてデジタル庁と協議の上で決定すること。

図表 3-1 納品成果物一覧（想定）

項番	成果物	内容	納入期限（想定）
1	中間報告書(サマリ)	本業務に係る作業状況の中間報告(サマリ)を記載したドキュメント。 作業着手後 3 カ月頃の提示を想定する。 詳細はデジタル庁と協議の上決定すること。	令和 5 年 6 月末～7 月初旬頃を想定
2	安全性評価結果報告書	本業務の実施内容及び安全性評価結果を記載した報告書。約 30 ページ程度を想定する。	本業務の完了時

(2) 納品方法

ア　受託者は、全ての納入成果物について、事前にデジタル庁のレビュー及び承認を受けてから、納期までに納品すること。そのため、実施スケジュールの調整時に、デジタル庁のレビュー及び指摘対応に要する期間を事前に調整にすること。

イ　受託者は、原則として、全ての納入成果物について、全て日本語で作成すること。ただし、情報処理に関する用語等、日本国においても英字で表記されることが一般的な文言については、英字のまま記載しても構わない。また、関連する引用資料等、日本語化が不能なものについても、英語若しくは英字のままの記載としても構わない。なお、用字・用語・記述符号の表記は「公用文作成の要領（昭和 27 年 4 月 4 日内閣閣甲第 16 号内閣官房長官依命通知）」に準拠すること。また、情報処理に関する用語の表記は、原則として日本産業規格（JIS）の規定に準拠すること。

ウ　受託者は、全ての納入成果物について、原則として電子データで作成すること。納入形態の詳細（電子媒体のファイル形式等も含む。）については、デジタル庁と協議の上、決定すること。

エ　受託者は、納入成果物のドキュメント類について、デジタル庁での確認を可能とするため、原則として Microsoft Word、Excel、PowerPoint 形式等のデジタル庁において閲覧・編集可能なファイル形式及び PDF 形式（ただし、PDF 形式は納入後に加除訂正等のない成果物に限る。）で作成すること。また、デジタル庁が他の形式による提出を求める場合は、協議の上対応方針を決定すること。

オ　受託者は、納入成果物の作成に当たり、ドキュメントに図表や写真を貼り付けている場合は、図表や写真のデータはアウトライン化・画像化せず、取り出せるデータとして埋込む又は別データとして格納すること。

カ　受託者は、成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。

キ　受託者は、提出した成果物に対してデジタル庁の検査を受けること。検査の結果、納入成果物の全部又は一部が不合格となった場合は、必要な対応を行った後、指定した期日までに改めて納品すること。

(3) 納品場所

原則として、成果物は次の場所において引渡しを行うこと。ただし、デジタル庁が納品場所を別途指示

する場合はこの限りではない。

〒102-0094

東京都千代田区紀尾井町 1-3 東京ガーデンテラス紀尾井町 19 階

デジタル庁 国民向けサービスグループ マイナンバーカード担当

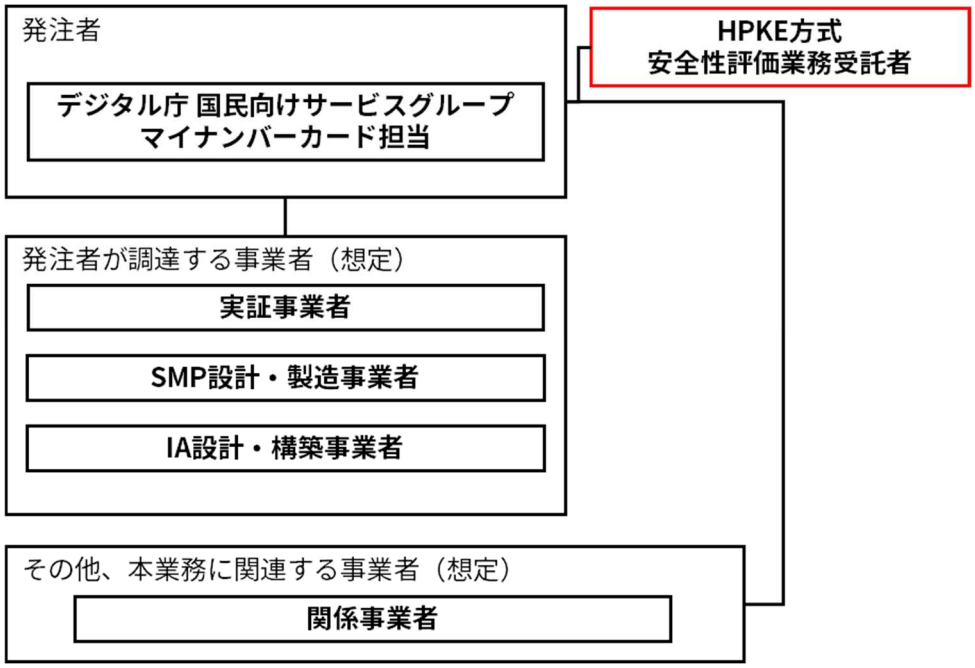
（TEL：03-4477-6775、E-Mail：mynumber_smartphone@digital.go.jp）

4. 作業の実施体制・方法に関する事項

4.1. 全体体制

本業務の実施に係る体制について、以下に示す。

図表 4-1 全体体制図



体制に記載されている関係組織の概要及び役割について、以下に示す。

図表 4-2 関係組織一覧

項番	区分	組織	概要及び役割
1	発注者	デジタル庁国民向けサービスグループ マイナンバーカード担当（PJMO）	• 本システムの設計、開発等を担当する。 • スマホJPKIシステム（SP-TSM等を含む）の設計、開発等を担当した。 • 本システム開発後の運用を担当する。
2	関連事業者	実証事業者	• 本システム及び SP-TSM 等の技術検証を実施する事業者。（調達済）
3		SMP 設計・製造事業者	• 本システムのうち SMP について、設計・製造を実施する事業者。（令和 5 年度調達済）
4		IA 設計・構築事業者	• 本システムのうち、IA について、設計・構築を実施する事業者（令和 5 年度調達済） • 設計事業者との役割分担は、要件定義書 別紙 6「システム関連図」を参照すること。

項番	区分	組織	概要及び役割
5		関係事業者	• 本業務における関係事業者
6	調査研究受託者	HPKE 方式安全性評価業務受託者（受託者）	• HPKE 暗号化方式における暗号の安全性ならびに鍵管理・鍵交換方式の運用面における堅牢性の評価・確認を行う業務の受託者（令和 6 年度調達予定）

4.2. **作業体制に求める要件**

受託者の作業体制に求める要件について、以下に示す。

(1) 業務実施者の適格性の確保等

業務実施者は以下の条件を満たすものとし、それらを示す書類を提出すること。

(ア) HPKE 暗号通信方式または E2EE 暗号通信方式に用いられている暗号プロトコルの評価実績を有しており、同暗号通信方式における基礎研究成果を論文等で発表していること。

(イ) HPKE 暗号通信方式または E2EE 暗号通信方針式に採用されている暗号化や復号の基本的な手順を実現する為のアルゴリズムについて解析を行った実績を有していること。

(ウ) 実際に市場に流通している製品・サービスの暗号システムに関する設計・解析経験を有しており、その設計・解析に関する実績を公表していること。

(2) 情報保全の履行体制

イ　この契約の履行に際し知り得た保護すべき情報（契約を履行する一環として受託者が収集、整理、作成等した情報であって、デジタル庁が保護を要さないと確認したものを除く。）及びその他の非公知の情報（デジタル庁から提供した情報を含む。以下「保護すべき情報等」という。）について、適切に管理するものとする。

ウ　保護すべき情報等の取扱いについては、次の履行体制を確保し、これを変更した場合には、遅滞なくデジタル庁に通知するものとする。

(ア) デジタル庁が保護を要さないと確認するまでは保護すべき情報として取り扱う履行体制

(イ) デジタル庁の同意を得て指定した取扱者以外の者に取扱わせない履行体制

(ウ) デジタル庁が許可した場合を除き、受託者に対して指導、監督、業務支援、助言、監査等を行う者を含む一切の受託者以外の者に対して伝達又は漏えいさせない履行体制

エ　契約の履行中、履行後を問わず情報の漏洩等の事故や疑い、将来的な懸念の指摘があったときは、直ちに必要な措置等を講ずるとともに、デジタル庁に報告すること。また、デジタル庁から求められた場合は、情報の管理の履行状況等を報告するとともに、デジタル庁による調査が行われる場合は、これに協力すること。

4.3. **作業の管理に関する要領**

本業務の作業の管理状況について、デジタル庁からの確認要請があった場合は、デジタル庁への報告を実施すること。

5. 作業の実施に当たっての遵守事項

5.1. 機密保持、資料の取扱い

ア　受託者は、本業務に関してデジタル庁が開示した情報（公知の情報等を除く。以下同じ。）、契約履行過程で生じた納入成果物に関する情報、その他当該業務の実施において知り得た情報について、本業務の目的以外に使用または第三者に開示若しくは漏洩してはならないものとし、そのために必要な措置を講ずること。当該情報を本業務以外の目的に使用または第三者に開示する必要がある場合、事前にデジタル庁の承認を得ること。

イ　受託者は、本業務の遂行における情報セキュリティ対策の履行が不十分である可能性をデジタル庁が認める場合には、デジタル庁の求めに応じ協議を行い、合意した対応を取ること。

ウ　受託者は、本調達に係る業務の実施のためにデジタル庁から提供する情報及び当該業務の実施において知り得た情報について、以下の事項を遵守すること。ただし、既に公知である情報については、この限りではない。

(ア)　本調達に係る業務にのみ使用し、他の目的には使用しないこと。

(イ)　本調達に係る業務を行う者以外には機密とすること。

エ　受託者は、本調達に係る業務の実施のために取得し、処理する要機密情報を、全て国内法が適用される場所に保存すること。

オ　受託者は、デジタル庁から、本調達に係る業務の遂行における情報セキュリティ対策の履行状況に関する以下の事項の報告を求められた場合は、速やかに回答すること。

(ア)　受託者に取り扱わせるデジタル庁の情報の機密保持等に係る管理状況

5.2. 遵守する法令等

(1) 法令などの遵守

受託者は、本業務の実施に当たり、以下の法令等を遵守すること。

ア　民法（明治 29 年法律第 89 号）

イ　刑法（明治 40 年法律第 45 号）

ウ　私的独占の禁止及び公正取引の確保に関する法律（昭和 22 年法律第 54 号）

エ　著作権法（昭和 45 年法律第 48 号）

オ　不正アクセス行為の禁止等に関する法律（平成 11 年法律 128 号）

カ　行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号）

キ　電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成 14 年法律第 153 号）

ク　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）

また、上記以外にも関連する法令等がある場合は、遵守すること。

6. 成果物に関する事項

6.1. 知的財産権の帰属

ア　本業務における成果物の原著作権及び二次的著作物の著作権（著作権法第 21 条から第 28 条までに定める全ての権利を含む。）は、受託者が本調達の実施の従前から権利を保有していた等の明確な理由によりあらかじめ提案書にて権利譲渡不可能と示されたもの以外は、全てデジタル庁に帰属するものとする。

イ　デジタル庁は、成果物について、第三者に権利が帰属する場合を除き、自由に複製し、改変等し、及びそれらの利用を第三者に許諾することができるとともに、任意に開示できるものとする。

ウ　納品される成果物に第三者が権利を有する著作物（以下「既存著作物等」という。）が含まれる場合には、受託者は、当該既存著作物等の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続を行うこと。この場合、本業務の受託者は、当該既存著作物の内容について事前にデジタル庁の承認を得ることとし、デジタル庁は、既存著作物等について当該許諾条件の範囲で使用するものとする。なお、本仕様に基づく作業に関し、第三者との間に著作権に係る権利侵害の紛争の原因が専らデジタル庁の責めに帰す場合を除き、受託者の責任及び負担において一切を処理すること。この場合、デジタル庁は係る紛争等の事実を知ったときは、受託者に通知し、必要な範囲で訴訟上の防衛を受託者に委ねる等の協力措置を講じるものとする。

エ　本業務における成果物の著作権や、本評価に関する学会への発表の可否はデジタル庁と協議の上決定することとする。

オ　本件の成果物に係る所有権は、デジタル庁から受託者に対価が完済されたとき、受託者からデジタル庁に移転するものとする。

カ　受託者はデジタル庁に対し、一切の著作者人格権を行使しないものとし、また、第三者をして行使させないものとする。また、受託者が本受託業務の実施の過程で生じた納入成果物に係る著作権を自ら使用し又は第三者をして使用させる場合は、デジタル庁と別途協議するものとする。

キ　受託者は使用する画像、デザイン、表現等に関して他者の著作権を侵害する行為に十分配慮し、これを行わないこと。

7. その他特記事項

本業務に関連するその他特記事項について、以下に示す。

ア　本業務を実施する上で必要と判断する諸経費については、受託者が関係者と調整し、予め見積りに含めること。

イ　本仕様書の内容及び解釈等について不明な個所がある場合、その他特に必要がある場合は、事前にデジタル庁と協議し、決定、解決すること。この場合、当該協議に関する議事録を作成し、デジタル庁の確認を受けること。

ウ　本業務受託後に、本調達仕様書の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもってデジタル庁に申し入れを行うこと。双方の協議において、その変更内容が軽微（委託料、納期に影響を及ぼさない）かつ許容できると判断された場合は、変更の内容、理由等を明記した書面に双方が記名捺印することによって変更を確定する。

エ　本業務に係る費用は、業務完了後、契約書に定めるところにより支払うものとする。

オ　本業務における成果物の著作権や、本評価に関する学会への発表の可否はデジタル庁と協議の上決定することとする。