Deloitte.
デロイト トーマツ

トーマツ.
有限責任監査法人トーマツ
〒100-8360
東京都千代田区丸の内三丁目2番3号
丸の内二重橋ビルディング
Tel：(03) 6213-1000

独立した監査法人の認証局のための WebTrust 保証報告書

令和 7 年 7 月 23 日

デジタル庁　デジタル社会共通機能グループ
企画官　　千葉　英之　殿

有限責任監査法人トーマツ
社員　公認会計士　野坂 晃史

範囲

有限責任監査法人トーマツ（以下「当監査法人」という。）は、認証局のための WebTrust の規準 v2.2.2（the WebTrust Principles and Criteria for Certification Authorities v2.2.2）に基づいて、令和 6 年 6 月 1 日から令和 7 年 5 月 31 日までの期間において、付録 A に記載された政府認証基盤の認証局（以下「CA」という。）のサービス（東京）（以下「CA サービス」という。）に関する経営者の記述書について合理的保証業務を実施した。

経営者の記述書によれば、政府認証基盤は CA サービスについて、下記事項を実施していた。

- 政府認証基盤は、CA が実施するビジネス、鍵のライフサイクル管理と証明書のライフサイクル管理及び CA 環境管理の実務を、政府認証基盤の Web サイトで付録 B に記載された証明書ポリシー/認証局運用規程にて開示していた。
- 政府認証基盤は、下記について合理的な保証を提供する有効な内部統制を維持していた。
  - 政府認証基盤は、証明書ポリシー/認証局運用規程に準拠してサービスを提供していたこと。
- 政府認証基盤は、下記について合理的な保証を提供する有効な内部統制を維持していた。
  - 政府認証基盤が管理する鍵と証明書のインテグリティが確立され、そのライフサイクルを通じて保護されていたこと。
  - 政府認証基盤が管理する加入者鍵及び加入者証明書のインテグリティが確立され、そのライフサイクルを通じて保護されていたこと。
  - 加入者の情報は、（政府認証基盤が行う登録業務のため）適切に認証されていたこと。
- 政府認証基盤は、下記について合理的な保証を提供する有効な内部統制を維持していた。
  - CA システム及びデータへの論理的、物理的アクセスは、承認された個人に制限されていたこと。
  - 鍵と証明書の管理に関する運用の継続性が維持されていたこと。
  - CA システムのインテグリティを維持するため、CA システムの開発、保守及び運用が適切に承認され、実施されていたこと。

政府認証基盤は、CA 鍵のアーカイブ、寄託及びマイグレーションを行わず、加入者鍵の復旧サービス、鍵更新を伴わない証明書の更新サービス、証明書の一時停止サービス及び第三者の下位 CA 又はクロス証明書の発行・管理を提供しない。したがって、当監査法人の手続は、それらの規準に関連する内部統制を含んでいない。

認証局の責任

政府認証基盤の経営者の責任は、認証局のための WebTrust の規準 v2.2.2 に準拠して、経営者の記述書を適正に作成すること及び記述書に記載されたサービスを提供することにある。

職業倫理、独立性及び品質管理

当監査法人は、誠実性、客観性、職業的専門家としての能力及び正当な注意、秘密保持並びに職業的専門家としての行動に関する基本原則を基礎とする国際会計士倫理基準審議会の職業会計士のための国際倫理規程（Code of Ethics for Professional Accountants、国際独立性基準を含む。）の独立性及びその他の職業倫理に関する規定を遵守している。

また、当監査法人は、国際品質マネジメント基準（Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements）の第 1 号を適用しており、したがって、職業倫理に関する規定、職業的専門家としての基準及び適用される法令等の要求事項の遵守に関して文書化した方針と手続を含む、包括的な品質管理システムを維持している。

業務実施者の責任

当監査法人の責任は、当監査法人の実施した手続に基づき、経営者の記述書について意見を表明することにある。

当監査法人は、国際監査・保証基準審議会が公表した国際保証業務基準 3000「過去財務情報の監査又はレビュー以外の保証業務（Assurance Engagements Other than Audits or Reviews of Historical Financial Information）」に準拠して業務を実施した。当該基準は当監査法人に、全ての重要な点において、経営者の記述書が適正に表示されているかどうかについて、合理的な保証を得るための手続を計画し、実施することを求めている。したがって、手続には以下が含まれる。

1. 政府認証基盤の鍵と証明書のライフサイクル管理のビジネス実務及び鍵と証明書のインテグリティ、加入者と信頼者情報の認証と機密保持、鍵と証明書のライフサイクル管理に係る運用の継続性、システムインテグリティの開発、保守及び運用に関する内部統制を理解すること。
2. 政府認証基盤が開示した鍵と証明書のライフサイクル管理のビジネス実務に従って実施された取引を試査によりテストすること。
3. 内部統制の運用評価手続を実施し、評価すること。
4. 当監査法人が状況に応じて必要と認めたその他の手続を実施すること。

当監査法人は、意見表明のための基礎となる十分かつ適切な証拠を得たと判断している。

政府認証基盤の CA サービスにおける特定の内部統制の相対的な有効性と重要性及び加入者と信頼者の内部統制リスクの評価に与える影響は、内部統制との相互作用及び個々の加入者と信頼者の所在場所において現れるその他の要因に依存している。当監査法人は個別の加入者と信頼者の所在場所における内部統制の有効性を評価するための手続を実施していない。

内部統制の限界

内部統制の性質や固有の限界のため、先に述べた規準に適合するための政府認証基盤の能力に影響を及ぼす可能性がある。例えば、内部統制により誤びゅう又は不正、システムや情報への未承認のアクセス、社内及び外部のポリシーや要求への遵守性違反を防止又は発見、修正することができない可能性がある。また、当監査法人の発見事項に基づく結論から将来を予測することは、変更が生ずることにより、その結論の妥当性を失うリスクがある。

Deloitte.
デロイト トーマツ

トーマツ.

意見

当監査法人は、経営者の記述書が、認証局のための WebTrust の規準 v2.2.2 に基づいて、令和 6 年 6 月 1 日から令和 7 年 5 月 31 日までの期間において、全ての重要な点において適正に表示されているものと認める。

この保証報告書は、認証局のための WebTrust の規準 v2.2.2 が対象としている範囲を超えて、政府認証基盤の CA サービスの品質について何ら表明するものではない。また、いかなる顧客の意図する目的に対する政府認証基盤の CA サービスの適合性についても何ら表明するものではない。

WebTrust シールの使用

政府認証基盤の認証局のための WebTrust シールの使用は、この保証報告書の内容を象徴的に表示しているが、この保証報告書の変更又は追加的な保証を提供することを意図したものではなく、そのような解釈をすべきではない。

以上

付録 A　対象 CA の識別情報

CA#	日本政府ルート認証局
Cert#	自己署名証明書
サブジェクト	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
発行者	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
シリアル番号	311EE08CBA24583B6199AA
キーアルゴリズム	ECDSA
キーサイズ	384 ビット
ダイジェストアルゴリズム	SHA384
有効期限の開始	2023年12月13日　0:00:00 JST
有効期限の終了	2048年12月12日　23:59:59 JST
サブジェクトキー識別子	76AF9B2EB0116F4F1E430E81C0F39FED26FABEC1
フィンガープリント　SHA-1	4DCF7D1B9B2608ED2C96B66B29610FCEE76AC7F4
フィンガープリント　SHA-256	D7A5514D93F7D53BD27DE2051F8E1FF71CA0AC78FACFE46A8BCCA4589984AE64

Deloitte.
デロイト トーマツ

トーマツ.

CA#	官職サブ認証局
Cert#	中間認証局証明書
サブジェクト	CN = OfficialStatus Sub CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
発行者	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
シリアル番号	38B3C6FD0D1C58CFE4CA9C
キーアルゴリズム	ECDSA
キーサイズ	384 ビット
ダイジェストアルゴリズム	SHA384
有効期限の開始	2023年12月13日 0:00:00 JST
有効期限の終了	2038年12月12日 23:59:59 JST
サブジェクトキー識別子	8E7AA9C33B31B696727855B410566ADA843D78B7
フィンガープリント SHA-1	A437A572213AEB3EAF15AD5C97E1FFB46C6A1AE6
フィンガープリント SHA-256	FAD90EB633099ECF2BF227D0E4A71CD95773E68B21B6F436508D425B39901275

Deloitte.
デロイト トーマツ

トーマツ.

CA#	組織サブ認証局
Cert#	中間認証局証明書
サブジェクト	CN = Organization Sub CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
発行者	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
シリアル番号	3139CC50BD18014D66750F89
キーアルゴリズム	ECDSA
キーサイズ	384 ビット
ダイジェストアルゴリズム	SHA384
有効期限の開始	2024年7月17日 0:00:00 JST
有効期限の終了	2039年7月16日 23:59:59 JST
サブジェクトキー識別子	303C915AF4ADD2421FDFB245D97881ADDFC1B446
フィンガープリント SHA-1	A5C1EDA2EDD661E4DD19CEB947D50B1B1ABD9604
フィンガープリント SHA-256	DABBB7DD7C1186D9CF677B559C29DE50FA3DDA252BFB6B134A95659444A01458

付録 B　認証局運用規程及び証明書ポリシー

CA	CP/CPS 名	Version	日付
日本政府ルート認証局 官職サブ認証局 組織サブ認証局	政府認証基盤（GPKI）日本政府認証局 CP/CPS	第 1.03 版	2025 年（令和 7 年）5 月 23 日
	政府認証基盤（GPKI）日本政府認証局 CP/CPS	第 1.02 版	2025 年（令和 7 年）1 月 27 日
	政府認証基盤（GPKI）日本政府認証局 CP/CPS	第 1.01 版	2024 年（令和 6 年）6 月 20 日
	政府認証基盤（GPKI）日本政府認証局 CP/CPS	第 1.00 版	2023 年（令和 5 年）12 月 8 日

経営者の記述書

令和 7 年 7 月 23 日

デジタル庁　デジタル社会共通機能グループ
企画官
千葉 英之

当認証基盤は、付録 A に記載された認証局（以下「CA」という。）を運営し、次の認証局サービス（以下「CA サービス」という。）を提供している。

- 加入者の登録
- 鍵更新を伴う証明書の更新
- 証明書の発行
- 証明書の配布
- 証明書の失効
- 証明書の検証
- 加入者鍵の生成と管理

当認証基盤の経営者は、当認証基盤の Web サイトで公開している CA ビジネス実務の開示、CA ビジネス実務管理、CA 環境の内部統制、CA 鍵ライフサイクル管理の内部統制、加入者鍵ライフサイクル管理の内部統制及び証明書ライフサイクル管理の内部統制を含む当認証基盤の CA の運用について、有効な内部統制を確立し、維持することに責任がある。これらの内部統制はモニタリングの仕組みを含んでおり、識別された欠陥を修正するための行動が取られる。

内部統制には誤びゅう及び内部統制の迂回又は無視を含む固有の限界がある。したがって、有効な内部統制といえども、当認証基盤の CA の運用について合理的な保証を提供するものでしかない。さらに、状況の変化により、内部統制の有効性は時間とともに変化する場合がある。

当認証基盤の経営者は、当認証基盤の CA（東京）の運用に関するビジネス実務の開示と内部統制を評価した。その評価に基づく当認証基盤の経営者の意見では、当認証基盤は、認証局のための WebTrust の規準 v2.2.2（the WebTrust Principles and Criteria for Certification Authorities v2.2.2）に準拠して、令和 6 年 6 月 1 日から令和 7 年 5 月 31 日までの期間において、CA サービスの提供に関して、下記の事項を実施した。

- 当認証基盤は、CA が実施するビジネス、鍵のライフサイクル管理と証明書のライフサイクル管理及び CA 環境管理の実務を、当認証基盤の Web サイトで付録 B に記載された証明書ポリシー/認証局運用規程にて開示していた。
- 下記について合理的な保証を提供する有効な内部統制を維持していた。
  - 当認証基盤は、（各 CA の）証明書ポリシー/認証局運用規程に準拠してサービスを提供していたこと。
- 下記について合理的な保証を提供する有効な内部統制を維持していた。
  - 当認証基盤が管理する鍵と証明書のインテグリティが確立され、そのライフサイクルを通じて保護されていたこと。
  - 当認証基盤が管理する加入者鍵と加入者証明書のインテグリティが確立され、そのライフサイクルを通じて保護されていたこと。
  - 加入者の情報は、（当認証基盤が行う登録業務のため）適切に認証されていたこと。

- 下記について合理的な保証を提供する有効な内部統制を維持していた。
  - CA システムとデータへの論理的、物理的アクセスは、承認された個人に制限されていたこと。
  - 鍵と証明書の管理に関する運用の継続性が維持されていたこと。
  - CA システムのインテグリティを維持するため、CA システムの開発、保守及び運用が適切に承認され、実施されていたこと。

当認証基盤が準拠した認証局のための WebTrust の規準 v2.2.2 には、以下が含まれる。

CA ビジネス実務の開示

- 認証局運用規程（CPS）

CA ビジネス実務管理

- 認証局運用規程の管理

CA 環境の内部統制

- セキュリティ管理
- 資産の分類と管理
- 人員のセキュリティ
- 物理的・環境的セキュリティ
- 運用管理
- システムアクセス管理
- システム開発と保守
- ビジネス継続性の管理
- モニタリングと遵守
- 監査ログの取得

CA 鍵ライフサイクル管理の内部統制

- CA 鍵の生成
- CA 鍵のストレージ、バックアップと復旧
- CA 公開鍵の配布
- CA 鍵の使用法
- CA 鍵の破棄
- CA 鍵の危殆化
- CA 暗号化ハードウェアライフサイクル管理

加入者鍵ライフサイクル管理の内部統制

- CA が提供する加入者鍵生成サービス
- CA が提供する鍵保存サービス
- IC カード（ICC）ライフサイクル管理
- 加入者鍵管理の要件

証明書ライフサイクル管理の内部統制

- 加入者の登録
- 鍵更新を伴う証明書の更新
- 証明書の発行
- 証明書の配布

- 証明書の失効
- 証明書の検証

当認証基盤は、CA 鍵のアーカイブ、寄託及びマイグレーションを行わず、加入者鍵の復旧サービス、鍵更新を伴わない証明書の更新サービス、証明書の一時停止サービス及び第三者の下位 CA 又はクロス証明書の発行・管理を提供しない。したがって、当認証基盤の記述書には、それらの規準に関連する内部統制を含んでいない。

以上

付録 A　対象 CA の識別情報

CA#	日本政府ルート認証局
Cert#	自己署名証明書
サブジェクト	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
発行者	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
シリアル番号	311EE08CBA24583B6199AA
キーアルゴリズム	ECDSA
キーサイズ	384 ビット
ダイジェストアルゴリズム	SHA384
有効期限の開始	2023年12月13日　0:00:00 JST
有効期限の終了	2048年12月12日　23:59:59 JST
サブジェクトキー識別子	76AF9B2EB0116F4F1E430E81C0F39FED26FABEC1
フィンガープリント　SHA-1	4DCF7D1B9B2608ED2C96B66B29610FCEE76AC7F4
フィンガープリント　SHA-256	D7A5514D93F7D53BD27DE2051F8E1FF71CA0AC78FACFE46A8BCCA4589984AE64

CA#	官職サブ認証局
Cert#	中間認証局証明書
サブジェクト	CN = OfficialStatus Sub CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
発行者	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
シリアル番号	38B3C6FD0D1C58CFE4CA9C
キーアルゴリズム	ECDSA
キーサイズ	384 ビット
ダイジェストアルゴリズム	SHA384
有効期限の開始	2023年12月13日 0:00:00 JST
有効期限の終了	2038年12月12日 23:59:59 JST
サブジェクトキー識別子	8E7AA9C33B31B696727855B410566ADA843D78B7
フィンガープリント SHA-1	A437A572213AEB3EAF15AD5C97E1FFB46C6A1AE6
フィンガープリント SHA-256	FAD90EB633099ECF2BF227D0E4A71CD95773E68B21B6F436508D425B39901275

CA#	組織サブ認証局
Cert#	中間認証局証明書
サブジェクト	CN = Organization Sub CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
発行者	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
シリアル番号	3139CC50BD18014D66750F89
キーアルゴリズム	ECDSA
キーサイズ	384 ビット
ダイジェストアルゴリズム	SHA384
有効期限の開始	2024年7月17日 0:00:00 JST
有効期限の終了	2039年7月16日 23:59:59 JST
サブジェクトキー識別子	303C915AF4ADD2421FDFB245D97881ADDFC1B446
フィンガープリント SHA-1	A5C1EDA2EDD661E4DD19CEB947D50B1B1ABD9604
フィンガープリント SHA-256	DABBB7DD7C1186D9CF677B559C29DE50FA3DDA252BFB6B134A95659444A01458

付録 B　認証局運用規程及び証明書ポリシー

CA	CP/CPS 名	Version	日付
日本政府ルート認証局 官職サブ認証局 組織サブ認証局	政府認証基盤（GPKI）日本政府認証局 CP/CPS	第 1.03 版	2025 年（令和 7 年）5 月 23 日
	政府認証基盤（GPKI）日本政府認証局 CP/CPS	第 1.02 版	2025 年（令和 7 年）1 月 27 日
	政府認証基盤（GPKI）日本政府認証局 CP/CPS	第 1.01 版	2024 年（令和 6 年）6 月 20 日
	政府認証基盤（GPKI）日本政府認証局 CP/CPS	第 1.00 版	2023 年（令和 5 年）12 月 8 日

Deloitte Touche Tohmatsu LLC
Marunouchi Nijubashi Building
3-2-3 Marunouchi
Chiyoda-ku, Tokyo, 100-8360
Japan
Tel: +81 (3) 6213 1000

INDEPENDENT ASSURANCE REPORT

23 July 2025

To Mr. Hideyuki Chiba
Director for Policy Planning
Group of Common Functions for Digital Society
Government of Japan, Digital Agency

Koji Nosaka
Partner
Tokyo Office
Deloitte Touche Tohmatsu LLC

Scope

We have been engaged, in a reasonable assurance engagement, to report on GPKI management's assertion that for its Certification Authority (CA) operations at Tokyo, Japan, throughout the period of 1 June 2024 to 31 May 2025 for its CAs as enumerated in Appendix A, GPKI has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certificate Policies / Certification Practice Statements (CP/CPS) as enumerated in Appendix B on GPKI's website
- maintained effective controls to provide reasonable assurance that:
  - GPKI provides its services in accordance with its CP/CPS
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles; and
  - subscriber information is properly authenticated (for the registration activities performed by GPKI)
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

GPKI does not perform CA keys archiving, escrow, and migration. GPKI does not provide subscriber key recovery services,

certificate renewal services, suspension services, and third-party subordinate CA or cross-certificate issuance or management. Accordingly, our procedures did not extend to controls that would address those criteria.

Certification authority's responsibilities

GPKI's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Our independence and quality management

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of GPKI's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
2. selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
3. testing and evaluating the operating effectiveness of the controls; and
4. performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at GPKI and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party location.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Deloitte.
デロイト トーマツ

Opinion

In our opinion, throughout the period of 1 June 2024 to 31 May 2025, GPKI management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

This report does not include any representation as to the quality of GPKI's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.2.2, nor the suitability of any of GPKI's services for any customer's intended purpose.

Use of the WebTrust seal

GPKI's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

(The above represents a translation, for convenience only, of the original report issued in the Japanese language.)

Deloitte.
デロイト トーマツ

Appendix A　CA Identifying Information for in Scope CAs

CA#	Japanese Government Root CA
Cert#	Self-signed certificate
Subject	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
Issuer	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
Serial	311EE08CBA24583B6199AA
Key Algorithm	ECDSA
Key Size	384bits
Digest Algorithm	SHA384
Not Before	13 December 2023, 0:00:00 JST
Not After	12 December 2048, 23:59:59 JST
SKI	76AF9B2EB0116F4F1E430E81C0F39FED26FABEC1
SHA1 Fingerprint	4DCF7D1B9B2608ED2C96B66B29610FCEE76AC7F4
SHA256 Fingerprint	D7A5514D93F7D53BD27DE2051F8E1FF71CA0AC78FACFE46A8BCCA4589984AE64

CA#	OfficialStatus Sub CA
Cert#	Intermediate CA certificate
Subject	CN = OfficialStatus Sub CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
Issuer	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
Serial	38B3C6FD0D1C58CFE4CA9C
Key Algorithm	ECDSA
Key Size	384bits
Digest Algorithm	SHA384
Not Before	13 December 2023, 0:00:00 JST
Not After	12 December 2038, 23:59:59 JST
SKI	8E7AA9C33B31B696727855B410566ADA843D78B7
SHA1 Fingerprint	A437A572213AEB3EAF15AD5C97E1FFB46C6A1AE6
SHA256 Fingerprint	FAD90EB633099ECF2BF227D0E4A71CD95773E68B21B6F436508D425B39901275

Deloitte.
デロイト トーマツ

CA#	Organization Sub CA
Cert#	Intermediate CA certificate
Subject	CN = Organization Sub CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
Issuer	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
Serial	3139CC50BD18014D66750F89
Key Algorithm	ECDSA
Key Size	384bits
Digest Algorithm	SHA384
Not Before	17 July 2024, 0:00:00 JST
Not After	16 July 2039, 23:59:59 JST
SKI	303C915AF4ADD2421FDFB245D97881ADDFC1B446
SHA1 Fingerprint	A5C1EDA2EDD661E4DD19CEB947D50B1B1ABD9604
SHA256 Fingerprint	DABBB7DD7C1186D9CF677B559C29DE50FA3DDA252BFB6B134A95659444A01458

Deloitte.
デロイト トーマツ

Appendix B　Certification Practice Statements and Certificate Policies

CA	Certificate Policy / Certification Practice Statement Name	Version	Date
Japanese Government Root CA OfficialStatus Sub CA Organization Sub CA	Government Public Key Infrastructure (GPKI) Japanese Government Certification Authority CP/CPS	1.03	23 May 2025
	Government Public Key Infrastructure (GPKI) Japanese Government Certification Authority CP/CPS	1.02	27 January 2025
	Government Public Key Infrastructure (GPKI) Japanese Government Certification Authority CP/CPS	1.01	20 June 2024
	Government Public Key Infrastructure (GPKI) Japanese Government Certification Authority CP/CPS	1.00	8 December 2023

GPKI MANAGEMENT'S ASSERTION

23 July 2025

Hideyuki Chiba
Director for Policy Planning
Group of Common Functions for Digital Society
Government of Japan, Digital Agency

Government Public Key Infrastructure ("GPKI") operates the Certification Authority (CA) services as enumerated in Appendix A, and provides the following CA services:

- Subscriber registration
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management

The management of GPKI is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, and certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to GPKI's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

GPKI management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in GPKI management's opinion, in providing its Certification Authority (CA) services at Tokyo, Japan, throughout the period of 1 June 2024 to 31 May 2025, GPKI has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certificate Policies / Certification Practice Statements (CP/CPS) as enumerated in Appendix B on GPKI's website
- maintained effective controls to provide reasonable assurance that:
  - GPKI provides its services in accordance with its CP/CPS
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles; and
  - subscriber information is properly authenticated (for the registration activities performed by GPKI)
- maintained effective controls to provide reasonable assurance that:

- logical and physical access to CA systems and data is restricted to authorised individuals;
- the continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)

CA Business Practices Management

- Certification Practice Statement Management

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage Services
- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

GPKI does not perform CA keys archiving, escrow, and migration. GPKI does not provide subscriber key recovery services, certificate renewal services, suspension services, and third-party subordinate CA or cross-certificate issuance or management. Accordingly, our assertion does not extend to controls that would address those criteria.

(The above represents a translation, for convenience only, of the original report issued in the Japanese language.)

Appendix A CA Identifying Information for in Scope CAs

CA#	Japanese Government Root CA
Cert#	Self-signed certificate
Subject	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
Issuer	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
Serial	311EE08CBA24583B6199AA
Key Algorithm	ECDSA
Key Size	384bits
Digest Algorithm	SHA384
Not Before	13 December 2023, 0:00:00 JST
Not After	12 December 2048, 23:59:59 JST
SKI	76AF9B2EB0116F4F1E430E81C0F39FED26FABEC1
SHA1 Fingerprint	4DCF7D1B9B2608ED2C96B66B29610FCEE76AC7F4
SHA256 Fingerprint	D7A5514D93F7D53BD27DE2051F8E1FF71CA0AC78FACFE46A8BCCA4589984AE64

CA#	OfficialStatus Sub CA
Cert#	Intermediate CA certificate
Subject	CN = OfficialStatus Sub CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
Issuer	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
Serial	38B3C6FD0D1C58CFE4CA9C
Key Algorithm	ECDSA
Key Size	384bits
Digest Algorithm	SHA384
Not Before	13 December 2023, 0:00:00 JST
Not After	12 December 2038, 23:59:59 JST
SKI	8E7AA9C33B31B696727855B410566ADA843D78B7
SHA1 Fingerprint	A437A572213AEB3EAF15AD5C97E1FFB46C6A1AE6
SHA256 Fingerprint	FAD90EB633099ECF2BF227D0E4A71CD95773E68B21B6F436508D425B39901275

CA#	Organization Sub CA
Cert#	Intermediate CA certificate
Subject	CN = Organization Sub CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
Issuer	CN = Japanese Government Root CA 2.5.4.97 = NTRJP-8000012010038 O = Japanese Government C = JP
Serial	3139CC50BD18014D66750F89
Key Algorithm	ECDSA
Key Size	384bits
Digest Algorithm	SHA384
Not Before	17 July 2024, 0:00:00 JST
Not After	16 July 2039, 23:59:59 JST
SKI	303C915AF4ADD2421FDFB245D97881ADDFC1B446
SHA1 Fingerprint	A5C1EDA2EDD661E4DD19CEB947D50B1B1ABD9604
SHA256 Fingerprint	DABBB7DD7C1186D9CF677B559C29DE50FA3DDA252BFB6B134A95659444A01458

Appendix B Certification Practice Statements and Certificate Policies

CA	Certificate Policy / Certification Practice Statement Name	Version	Date
Japanese Government Root CA OfficialStatus Sub CA Organization Sub CA	Government Public Key Infrastructure (GPKI) Japanese Government Certification Authority CP/CPS	1.03	23 May 2025
	Government Public Key Infrastructure (GPKI) Japanese Government Certification Authority CP/CPS	1.02	27 January 2025
	Government Public Key Infrastructure (GPKI) Japanese Government Certification Authority CP/CPS	1.01	20 June 2024
	Government Public Key Infrastructure (GPKI) Japanese Government Certification Authority CP/CPS	1.00	8 December 2023