

## INDEPENDENT ACCOUNTANT'S REPORT

To the management of Microsoft Public Key Infrastructure Services ("MS PKI Services") :

### Scope

We have examined MS PKI Services management's [assertion](#) that for its Certification Authority ("CA") operations in the United States of America, and in Ireland, for its CAs as enumerated in [Attachment A](#), MS PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Certificate Policies and Certification Practice Statements as enumerated in [Attachment B](#)
- maintained effective controls to provide reasonable assurance that
  - MS PKI Services' Certification Practice Statements are consistent with its Certificate Policies; and
  - MS PKI Services provides its services in accordance with its Certificate Policies and Certification Practice Statements
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by MS PKI Services); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- 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

throughout the period May 1, 2024 to April 30, 2025 based on the [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#).

MS PKI Services does not escrow its CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, or integrated circuit card lifecycle management for subscribers, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

Subscriber key-related services provided by Microsoft outside of the CA operations performed by MS PKI Services are out of scope. Additionally, there are other CA hierarchies and PKI operations across Microsoft that are not managed by MS PKI services. These CA hierarchies and PKI operations are not in the scope of this examination, and this opinion does not extend to these services.

### Certification authority's responsibilities

MS PKI Services' 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.

### Practitioner's responsibilities

Our responsibility is to express an opinion on MS PKI Services management's assertion based on our examination. Our examination was conducted in accordance with AT-C Section 205, *Assertion-Based Examination Engagements*, established by the American Institute of Certified Public Accountants, and International Standard on Assurance Engagements ("ISAE") 3000, *Assurance Engagements Other Than Audits Or Reviews Of Historical Financial Information*. This standard requires that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

### **Our independence and quality control**

We are required to be independent and to meet other ethical responsibilities in accordance with the Code of Professional Conduct established by the American Institute of Certified Public Accountants (“AICPA”) and Code of Ethics for Professional Accountants (including International Independence Standards) issued by the International Ethics Standards Board of Accountants’ (“IESBA”). We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and the International Standards on Quality Management issued by the International Auditing and Assurance Standards Board (“IAASB”) and, accordingly, maintain a comprehensive system of quality control.

### **Relative effectiveness of controls**

The relative effectiveness and significance of specific controls at MS PKI Services 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. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

### **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.

### **Opinion**

In our opinion management’s assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of MS PKI Services’ services other than its CA operations in the United States of America, and in Ireland, nor the suitability of any of MS PKI Services’ services for any customer’s intended purpose.

### **Use of the WebTrust seal**

MS PKI Services’ 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.

*Deloitte & Touche LLP*

Deloitte & Touche LLP  
July 16, 2025

**ATTACHMENT A**

**LIST OF IN SCOPE CAs**

<b>Root CAs</b>
1. Microsoft Identity Verification Root Certificate Authority 2020
<b>Intermediate CAs</b>
2. Microsoft ID Verified Code Signing PCA 2021
3. Microsoft ID Verified CS AOC CA 01
4. Microsoft ID Verified CS AOC CA 02
5. Microsoft ID Verified CS EOC CA 01
6. Microsoft ID Verified CS EOC CA 02
<b>Timestamp Authority CA</b>
7. Microsoft Public RSA Timestamping CA 2020

CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
1	1	C=US O=Microsoft Corporation CN=Microsoft Identity Verification Root Certificate Authority 2020	C=US O=Microsoft Corporation CN=Microsoft Identity Verification Root Certificate Authority 2020	5498D2D1D45B1995481379C811C08799	RSA	sha384RSA	4/16/2020 18:36	4/16/2045 18:44	N/A	C87ED26A852A1BCA1998040727CF50104F68A8A2	5367F20C7ADE0E2BCA790915056D086B720C33C1FA2A2661ACF787E3292E1270	
2	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	C=US O=Microsoft Corporation CN=Microsoft Identity Verification Root Certificate Authority 2020	330000000787A334A37BA58E1C00000000007	RSA	sha384RSA	4/1/2021 20:05	4/1/2036 20:15	N/A	d94129b00f0f636cef69d7f5cd299ea4486a30e6	3D29798CC5D3F0644A7E0DC9CB1CADE523EA5E83B335109B605BFEEA7D5F5C1	
3	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS AOC CA 01	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	3300000007378C5BA1D9588CD400000000007	RSA	sha384RSA	4/13/2021 17:31	4/13/2026 17:31	N/A	e883c433d7dc9f0c9c769a0aa6d4df87a65e58ee	7EE1F718CAE6B4D25D10115A367D84B7704E06BD6F8B498825FD42C852574BE9	
4	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS AOC CA 02	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	330000000496504BD2DBEEC8880000000004	RSA	sha384RSA	4/13/2021 17:31	4/13/2026 17:31	N/A	244599a177902a7cc3ca83b06e6416842af82c67	E82D27596C5DDF9F11E8B6981F5D018211BF2580F0619E5954BAD400175F38D0	
5	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS EOC CA 01	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	33000000064A1AFACF05616A7400000000006	RSA	sha384RSA	4/13/2021 17:31	4/13/2026 17:31	N/A	769c367413d1907d615fb302eb80f4994ba53e85	2FAA1C92228D5A05E07BAECFAA365F90A9B2F2DD846B014AE95880BAC3A976BB	
6	1	C=US O=Microsoft Corporation CN=Microsoft ID Verified CS EOC CA 02	C=US O=Microsoft Corporation CN=Microsoft ID Verified Code Signing PCA 2021	3300000005FB7A5C321361DF5D00000000005	RSA	sha384RSA	4/13/2021 17:31	4/13/2026 17:31	N/A	659f51ce85687f2f8a4588aadda731bb1e0d005e	B96CCAB201048A0AC2BA07AEA08D6DBEEA1688F55380A369B14A7BE11AEF828D	
7	1	C=US O=Microsoft Corporation CN=Microsoft Public RSA Timestamping CA 2020	C=US O=Microsoft Corporation CN=Microsoft Identity Verification Root Certificate Authority 2020	3300000005E5CF0FF62EC98700000000005	RSA	sha384RSA	11/19/2020 20:32	11/19/2035 20:42	N/A	Time Stamping (1.3.6.1.5.5.7.3.8) 6B69283A352F486340CF7BD8AF49E93ED93DDB21	36E731CFA9BFD69DAFB643809F6DEC500902F7197DAEAAD86EA0159A2268A2B8	

ATTACHMENT B

LIST OF MS PKI SERVICES' CERTIFICATE POLICIES AND CERTIFICATION PRACTICE STATEMENTS

CP Name	Version	Date
<a href="#">Microsoft PKI Services Certificate Policy</a>	3.1.9	April 21, 2025
<a href="#">Microsoft PKI Services Certificate Policy</a>	3.1.8	July 21, 2024
<a href="#">Microsoft PKI Services Certificate Policy</a>	3.1.7	July 27, 2023

CPS Name	Version	Date
<a href="#">Microsoft PKI Services Third Party Certification Practice Statement</a>	1.0.4	July 21, 2024
<a href="#">Microsoft PKI Services Third Party Certification Practice Statement</a>	1.0.3	May 17, 2024
<a href="#">Microsoft PKI Services Third Party Certification Practice Statement</a>	1.0.2	May 22, 2023

## MICROSOFT PUBLIC KEY INFRASTRUCTURE SERVICES MANAGEMENT'S ASSERTION

Microsoft Public Key Infrastructure Services ("MS PKI Services") operates the Certification Authority ("CA") services as enumerated in [Attachment A](#), and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

The management of MS PKI Services 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, certificate lifecycle management controls, and subordinate CA 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 MS PKI Services' CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

MS PKI Services management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in MS PKI Services management's opinion, in providing its CA services in the United States of America, and in Ireland, MS PKI Services has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the applicable versions of its Certificate Policies and Certification Practice Statements as enumerated in Attachment B
- maintained effective controls to provide reasonable assurance that
  - MS PKI Services' Certification Practice Statements are consistent with its Certificate Policies; and
  - MS PKI Services provides its services in accordance with its Certificate Policies and Certification Practice Statements
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by MS PKI Services); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- 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

throughout the period May 1, 2024 to April 30, 2025 based on the [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#), including the following:

### CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

### CA Business Practices Management

- Certification Practice Statement Management
- Certificate Policy Management
- CP and CPS Consistency

### **CA Environmental Controls**

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and 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 Archival
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

### **Subscriber Key Lifecycle Management Controls**

- Requirements for Subscriber Key Management

### **Certificate Lifecycle Management Controls**

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

### **Subordinate CA and Cross Certificate Lifecycle Management Controls**

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

MS PKI Services does not escrow its CA keys, does not provide subscriber key generation services, subscriber key storage and recovery services, or integrated circuit card lifecycle management for subscribers, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

Microsoft Public Key Infrastructure Services  
July 16, 2025

**ATTACHMENT A**

**LIST OF IN SCOPE CAs**

<b>Root CAs</b>
1. Microsoft Identity Verification Root Certificate Authority 2020
<b>Intermediate CAs</b>
2. Microsoft ID Verified Code Signing PCA 2021
3. Microsoft ID Verified CS AOC CA 01
4. Microsoft ID Verified CS AOC CA 02
5. Microsoft ID Verified CS EOC CA 01
6. Microsoft ID Verified CS EOC CA 02
<b>Timestamp Authority CA</b>
7. Microsoft Public RSA Timestamping CA 2020

ATTACHMENT B

LIST OF MS PKI SERVICES' CERTIFICATE POLICIES AND CERTIFICATION PRACTICE STATEMENTS

CP Name	Version	Date
<a href="#">Microsoft PKI Services Certificate Policy</a>	3.1.9	April 21, 2025
<a href="#">Microsoft PKI Services Certificate Policy</a>	3.1.8	July 21, 2024
<a href="#">Microsoft PKI Services Certificate Policy</a>	3.1.7	July 27, 2023

CPS Name	Version	Date
<a href="#">Microsoft PKI Services Third Party Certification Practice Statement</a>	1.0.4	July 21, 2024
<a href="#">Microsoft PKI Services Third Party Certification Practice Statement</a>	1.0.3	May 17, 2024
<a href="#">Microsoft PKI Services Third Party Certification Practice Statement</a>	1.0.2	May 22, 2023