

## 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 at locations enumerated in [Attachment C](#), 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 subscriber 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, 2025 to April 30, 2026 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.

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 unauthorized 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.

#### Emphasis of matters

Without modifying our opinion, we noted the following other matters during our procedures:

|   | Matter topic                                                      | Matter description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | <b>OCSP response formatting and infrastructure rollback issue</b> | <p>As publicly disclosed in Bugzilla <a href="#">1999850</a>, Microsoft PKI Services identified an issue in its new OCSP infrastructure where responses included fractional seconds in the 'thisUpdate', 'nextUpdate', and 'producedAt' fields, causing TLS handshake failures for some relying parties and creating inconsistency with RFC 5280. As a result, OCSP traffic was moved back to the legacy responder infrastructure while Microsoft works to remediate the issue and resume migration to the new environment.</p> <p>The Bugzilla ticket was closed as RESOLVED on July 1, 2026.</p> |

While the MS PKI Services management's [assertion](#) enumerates matters disclosed publicly on Mozilla's Bugzilla reporting system throughout the period May 1, 2025 to April 30, 2026, we have only noted those matters relevant to the CAs enumerated in [Attachment A](#) and applicable to the [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#).

#### 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 28, 2026

## ATTACHMENT A

### LIST OF IN SCOPE CAs

| Root CAs         |                                                                            |
|------------------|----------------------------------------------------------------------------|
| 1.               | AP Root Certificate Authority 2014                                         |
| 2.               | Azure Hardware Root Certificate Authority 2019                             |
| 3.               | Azure Sphere Root Certificate Authority 2020                               |
| 4.               | Microsoft Android Platform Root CA 2021                                    |
| 5.               | Microsoft Code Verification Root                                           |
| 6.               | Microsoft Corporation Third Party Marketplace Root                         |
| 7.               | Microsoft Development Root Certificate Authority 2014                      |
| 8.               | Microsoft ECC Development Root Certificate Authority 2018                  |
| 9.               | Microsoft ECC Devices Root CA 2023                                         |
| 10.              | Microsoft ECC Devices Root Certificate Authority 2017                      |
| 11.              | Microsoft ECC Services Root CA 2021                                        |
| 12.              | Microsoft ESRP Root Certificate Authority 2017                             |
| 13.              | Microsoft Mariner RSA Root CA 2023                                         |
| 14.              | Microsoft Mobile Root Certificate Authority 2015                           |
| 15.              | Microsoft Overlake Root Certificate Authority 2019                         |
| 16.              | Microsoft RSA Devices Root CA 2021                                         |
| 17.              | Microsoft RSA Devices Root CA 2023                                         |
| 18.              | Microsoft RSA Services Root CA 2021                                        |
| 19.              | Microsoft Services Federal Root 1                                          |
| 20.              | Microsoft Services Partner Root                                            |
| 21.              | Microsoft Supply Chain ECC Root CA 2022                                    |
| 22.              | Microsoft Supply Chain RSA Root CA 2022                                    |
| 23.              | Microsoft Surface Device Authentication Root CA 2014                       |
| 24.              | Microsoft TPM Root Certificate Authority 2014                              |
| 25.              | Microsoft Enterprise Identity Verification Root Certificate Authority 2020 |
| Intermediate CAs |                                                                            |
| 26.              | Azure RSA PS CA EOC CA 01                                                  |
| 27.              | Azure RSA PS CA EOC CA 02                                                  |
| 28.              | Azure RSA PS CS AOC CA 01                                                  |
| 29.              | Azure RSA PS CS AOC CA 02                                                  |
| 30.              | Azure RSA PS CS EOC CA 01                                                  |
| 31.              | Azure RSA PS CS EOC CA 02                                                  |
| 32.              | Azure RSA Public Services Code Signing PCA                                 |
| 33.              | Azure Services Linux Kmod PCA                                              |
| 34.              | ESRP0 RSA PCA 2017                                                         |
| 35.              | ESRP2 RSA PCA 2017                                                         |
| 36.              | IDNA SK PCA                                                                |
| 37.              | J2ME Manufacturer Domain CA 2015                                           |
| 38.              | J2ME Trusted Third Party Domain CA 2015                                    |
| 39.              | Linux Boot Loader Signing CA 2016                                          |
| 40.              | Lumia Labeling CA                                                          |
| 41.              | M365 RSA Services Code Signing PCA                                         |
| 42.              | Mariner Trusted Base RSA Code Signing CA                                   |
| 43.              | Microsoft Android Code Transparency and Upload PCA                         |
| 44.              | Microsoft Android Play App PCA                                             |
| 45.              | Microsoft Andromeda Attestation CA 2017                                    |
| 46.              | Microsoft Andromeda Attestation PCA 2017                                   |
| 47.              | Microsoft Andromeda Firmware Debug CA 2017                                 |
| 48.              | Microsoft Atlas Attestation CA 2020                                        |
| 49.              | Microsoft Atlas Attestation PCA 2020                                       |
| 50.              | Microsoft Atlas Firmware Debug CA 2020                                     |
| 51.              | Microsoft Band Firmware CA 2015                                            |
| 52.              | Microsoft Band Firmware Debug CA 2016                                      |

53. Microsoft Benham Attestation CA
54. Microsoft Benham Attestation PCA
55. Microsoft Cerberus AOC CA 01
56. Microsoft Cerberus AOC CA 02
57. Microsoft Cerberus EOC CA 01
58. Microsoft Cerberus EOC CA 02
59. Microsoft Cloud Server AOC CA 01
60. Microsoft Cloud Server AOC CA 02
61. Microsoft Cloud Server EOC CA 01
62. Microsoft Cloud Server EOC CA 02
63. Microsoft Corporation KEK 2K CA 2023
64. Microsoft Corporation KEK 3K CA 2023
65. Microsoft Corporation KEK 4K CA 2023
66. Microsoft Corporation KEK CA 2011
67. Microsoft Corporation Third Party Marketplace PCA
68. Microsoft Corporation UEFI CA 2011
69. Microsoft Corsica AOC CA 01
70. Microsoft Corsica AOC CA 02
71. Microsoft Corsica EOC CA 01
72. Microsoft Corsica EOC CA 02
73. Microsoft Development PCA 2014
74. Microsoft Devices OEM Code Sign CA 2018
75. Microsoft Devices UEFI CA 2016
76. Microsoft ECC Development PCA 2018
77. Microsoft ECC LFF Platform Attestation CA
78. Microsoft ECC LFF Platform Attestation PCA
79. Microsoft ECC NFF Platform Attestation CA
80. Microsoft ECC NFF Platform Attestation PCA
81. Microsoft ECC Surface Accessory Firmware CA 2018
82. Microsoft ECC Surface Accessory Firmware CA 2023
83. Microsoft ECC Third Party PCA 2019
84. Microsoft HoloLens Attestation CA 2018
85. Microsoft HoloLens Attestation PCA 2018
86. Microsoft HoloLens Firmware Debug CA 2018
87. Microsoft IDNA RSA Policy Signing CA
88. Microsoft IoT Hardware AOC CA 01
89. Microsoft IoT Hardware AOC CA 02
90. Microsoft IoT Hardware EOC CA 01
91. Microsoft IoT Hardware EOC CA 02
92. Microsoft Mobile Development PCA 2014
93. Microsoft Mobile PCA 2015
94. Microsoft OEM Custom CA 2014
95. Microsoft Option ROM UEFI CA 2023
96. Microsoft Overlake Agent Signing PCA 2019
97. Microsoft Overlake Celestial Peak AOC CA 01
98. Microsoft Overlake Celestial Peak AOC CA 02
99. Microsoft Overlake Celestial Peak EOC CA 01
100. Microsoft Overlake Celestial Peak EOC CA 02
101. Microsoft Overlake OS Signing PCA 2019
102. Microsoft Overlake Policy Signing PCA 2020
103. Microsoft Overlake STOS Signing PCA 2020
104. Microsoft Pinewood Attestation CA 2019
105. Microsoft Pinewood Attestation PCA 2019
106. Microsoft RSA Third Party PCA 2023
107. Microsoft SCD Claimants RSA CA
108. Microsoft SCD Products RSA CA
109. Microsoft SCD Systems RSA CA
110. Microsoft Secure Launch ECC PCA 2017

111. Microsoft Services Federal PCA 1  
112. Microsoft SH2 Firmware CA 2018  
113. Microsoft SH2 Firmware Debug CA 2018  
114. Microsoft Surface Accessories Windows Firmware CA 2013  
115. Microsoft Surface AFF Firmware CA 2021  
116. Microsoft Surface AFF Firmware Debug CA 2021  
117. Microsoft Surface AFF UEFI PK CA 2021  
118. Microsoft Surface Common Services CA 2014  
119. Microsoft Surface FFF Firmware CA 2018  
120. Microsoft Surface FFF Firmware Debug CA 2018  
121. Microsoft Surface for RT Firmware CA 2012  
122. Microsoft Surface for Windows 8 Pro Firmware CA 2012  
123. Microsoft Surface for Windows RT CA 2012  
124. Microsoft Surface for Windows RT EK Issuing CA 01  
125. Microsoft Surface for Windows RT EK Issuing CA 02  
126. Microsoft Surface for Windows RT EK Issuing CA 03  
127. Microsoft Surface for Windows RT EK Issuing CA 04  
128. Microsoft Surface Ganymede Attestation CA 2017  
129. Microsoft Surface Ganymede Attestation PCA 2017  
130. Microsoft Surface Hub Firmware CA 2015  
131. Microsoft Surface Hub UEFI PK CA 2015  
132. Microsoft Surface LFF 3 Firmware CA 2016  
133. Microsoft Surface LFF 3 Firmware Debug CA 2016  
134. Microsoft Surface LFF 3 UEFI PK CA 2016  
135. Microsoft Surface LFF Firmware CA 2021  
136. Microsoft Surface LFF Firmware Debug CA 2021  
137. Microsoft Surface LFF UEFI PK CA 2021  
138. Microsoft Surface MoBB-1 Boot Core CA 2019  
139. Microsoft Surface MoBB-1 CA 2014  
140. Microsoft Surface NFF Firmware CA 2015  
141. Microsoft Surface NFF Firmware CA 2021  
142. Microsoft Surface NFF Firmware Debug CA 2015  
143. Microsoft Surface NFF Firmware Debug CA 2021  
144. Microsoft Surface NFF UEFI PK CA 2015  
145. Microsoft Surface NFF UEFI PK CA 2021  
146. Microsoft Surface Services for Windows 8 Pro CA 2012  
147. Microsoft Surface Services for Windows RT CA 2012  
148. Microsoft Surface SFF Attestation CA 2013  
149. Microsoft Surface SFF Firmware CA 2013  
150. Microsoft Surface SFF Platform Key CA 2013  
151. Microsoft Surface SH2 Firmware CA 2022  
152. Microsoft Surface SH2 Firmware Debug CA 2022  
153. Microsoft Surface SH2 UEFI PK CA 2022  
154. Microsoft Surface Silicon Partner PCA 2018  
155. Microsoft Surface Stamps CA 2024  
156. Microsoft Surface with Windows RT v2 Boot ROM Fuse CA 2013  
157. Microsoft Surface with Windows RT v2 Firmware CA 2013  
158. Microsoft Surface with Windows RT v2 Platform Key CA 2013  
159. Microsoft Surface with Windows RT v2 Services Mobile CA 2013  
160. Microsoft Surface XLFF 2 Firmware CA 2016  
161. Microsoft Surface XLFF 2 Firmware Debug CA 2016  
162. Microsoft Surface XLFF 2 UEFI PK CA 2016  
163. Microsoft Surface XLFF Firmware CA 2021  
164. Microsoft Surface XLFF Firmware Debug CA 2021  
165. Microsoft Surface XLFF UEFI PK CA 2021  
166. Microsoft Surface XSFF Firmware CA 2018  
167. Microsoft Surface XSFF Firmware Debug CA 2018  
168. Microsoft Surface XSFF UEFI PK CA 2018

169. Microsoft UEFI CA 2023  
170. Microsoft Universal Store OnePay PCA 2015  
171. Microsoft VSMC PCA 2017  
172. Microsoft Windows Group Edition KEK CA 2015  
173. Microsoft Windows IoT KEK CA 2015  
174. Microsoft Windows IoT PCA 2015  
175. Microsoft Windows UEFI PK CA 2017  
176. Microsoft XCloud PCA 2018  
177. MR0 RSA PCA 2022  
178. MR1 RSA PCA 2022  
179. Phones UEFI CA 2016  
180. Surface Factory CA 2018  
181. Windows Hello 11B0C61D CA 2021  
182. Windows Hello 1767C8B4 CA 2018  
183. Windows Hello 19B92965 CA 2018  
184. Windows Hello 2096ADCC CA 2021  
185. Windows Hello 41738710 CA 2021  
186. Windows Hello 5CF190F8 CA 2018  
187. Windows Hello 73CA926A CA 2021  
188. Windows Hello 7BB5EEFC CA 2018  
189. Windows Hello 9F10CB1F CA 2021  
190. Windows Hello B5A8CEAC CA 2018  
191. Windows Hello FPR-I-256 CA 2023  
192. Windows Hello GD-256 CA 2023  
193. Windows Hello Secure Devices PCA 2018  
194. Windows Phone KEK CA 2012  
195. Microsoft Enterprise Identity Verification Code Signing PCA 2020  
196. Microsoft Enterprise Identity Verification WSCV PCA 2020  
197. Microsoft SCD Claimants ECC CA  
198. Microsoft SCD Products ECC CA  
199. Microsoft SCD Systems ECC CA  
200. Microsoft Enterprise ID Verification CS EOC CA 02  
201. Microsoft Enterprise ID Verification CS EOC CA 03  
202. Microsoft Enterprise ID Verification CS EOC CA 01  
203. Microsoft Enterprise ID Verification CS AOC CA 02  
204. Microsoft Enterprise ID Verification CS AOC CA 01  
205. Microsoft Enterprise ID Verification CS AOC CA 03  
206. Microsoft Enterprise ID Verification WSCV AOC CA 02  
207. Microsoft Enterprise ID Verification WSCV AOC CA 03  
208. Microsoft Enterprise ID Verification WSCV AOC CA 01  
209. Microsoft Enterprise ID Verification WSCV EOC CA 02  
210. Microsoft Enterprise ID Verification WSCV EOC CA 01  
211. Microsoft Enterprise ID Verification WSCV EOC CA 03

**ATTACHMENT B**

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

| <b>CP Name</b>                                            | <b>Version</b> | <b>Date</b>    |
|-----------------------------------------------------------|----------------|----------------|
| <a href="#">Microsoft PKI Services Certificate Policy</a> | 3.2.0          | April 20, 2026 |
| <a href="#">Microsoft PKI Services Certificate Policy</a> | 3.1.9          | April 21, 2025 |

| <b>CPS Name</b>                                                                   | <b>Version</b> | <b>Date</b>    |
|-----------------------------------------------------------------------------------|----------------|----------------|
| <a href="#">Microsoft PKI Services Corporate Certification Practice Statement</a> | 3.2.0          | April 20, 2026 |
| <a href="#">Microsoft PKI Services Corporate Certification Practice Statement</a> | 3.1.9          | April 21, 2025 |

**ATTACHMENT C**

**LIST OF MS PKI SERVICES' LOCATIONS IN-SCOPE**

| #  | Location Name                            | Location Type                                         | Location                 | In-Scope for Physical and Environmental Control Testing |
|----|------------------------------------------|-------------------------------------------------------|--------------------------|---------------------------------------------------------|
| 1  | Corporate headquarters and office spaces | Main office                                           | United States of America | No                                                      |
| 2  | Online CA hosting 1                      | Datacenter 1                                          | United States of America | Yes                                                     |
| 3  | Online CA hosting 2                      | Datacenter 2                                          | Ireland                  | Yes                                                     |
| 4  | Offline CA hosting 1                     | Primary offline CA facility                           | United States of America | Yes                                                     |
| 5  | Offline CA hosting 2                     | Disaster recovery / secondary offline CA facility     | United States of America | Yes                                                     |
| 6  | Secure storage 1                         | Secure storage for online CAs and offline CAs         | United States of America | Yes                                                     |
| 7  | Secure storage 2                         | Cold storage for online and offline CAs               | United States of America | Yes                                                     |
| 8  | Secure storage 3                         | Disaster recovery / secondary storage for offline CAs | United States of America | Yes                                                     |
| 9  | Secure storage 4                         | Third-party cold storage for offline CAs              | United States of America | Yes                                                     |
| 10 | Secure storage 5                         | Secure storage for online CAs and offline CAs         | Ireland                  | Yes                                                     |

## 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 Certification Authority ("CA") services at locations enumerated in [Attachment C](#), 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;
  - the integrity of subscriber 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, 2025 to April 30, 2026 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.

MS PKI Services has disclosed the following matters publicly on Mozilla's Bugzilla reporting system.

| Sr. | Bugzilla ID             | Bugzilla Title                                                                             | Created On     | Resolved On     | Status   |
|-----|-------------------------|--------------------------------------------------------------------------------------------|----------------|-----------------|----------|
| 1   | <a href="#">1962829</a> | Microsoft PKI Services: Policy document bug                                                | April 28, 2025 | April 25, 2026  | Resolved |
| 2   | <a href="#">1962830</a> | Microsoft PKI Services: Subscriber certificate change made that was not compliant with CPS | April 28, 2025 | June 20, 2025   | Resolved |
| 3   | <a href="#">1965612</a> | Microsoft PKI Services: Failure to Revoke in 5 Days for 1962829                            | May 9, 2025    | May 4, 2026     | Resolved |
| 4   | <a href="#">1970968</a> | Microsoft PKI Services: Incorrect Revocation Reason Code                                   | June 6, 2025   | July 8, 2025    | Resolved |
| 5   | <a href="#">1974592</a> | Microsoft PKI Services: Pre-Sign Linting Validation did not occur in ICA creation          | June 28, 2025  | August 30, 2025 | Resolved |

| Sr. | Bugzilla ID             | Bugzilla Title                                                                                              | Created On         | Resolved On       | Status   |
|-----|-------------------------|-------------------------------------------------------------------------------------------------------------|--------------------|-------------------|----------|
| 6   | <a href="#">1979475</a> | Microsoft PKI Services: End Entity Certificate Mis-issuance against CPS (BasicConstraints)                  | July 28, 2025      | January 20, 2026  | Resolved |
| 7   | <a href="#">1990801</a> | Microsoft: improper disclosure of CRL                                                                       | September 26, 2025 | November 3, 2025  | Resolved |
| 8   | <a href="#">1999850</a> | Microsoft PKI Services: OCSP Non-Compliance                                                                 | November 13, 2025  | July 1, 2026      | Resolved |
| 9   | <a href="#">2007221</a> | Microsoft PKI Services: Improper Disclosure of CRL                                                          | December 19, 2025  | March 2, 2026     | Resolved |
| 10  | <a href="#">2008847</a> | Microsoft PKI Services: Sample Site Certificates expired                                                    | January 7, 2026    | February 16, 2026 | Resolved |
| 11  | <a href="#">2009539</a> | Microsoft PKI Services: Improper Disclosure of CRLs – IDP – Existing CAs                                    | January 10, 2026   | February 16, 2026 | Resolved |
| 12  | <a href="#">2009541</a> | Microsoft PKI Services: Failure to report within 72 hrs - Sample Site Certs Expired                         | January 10, 2026   | February 11, 2026 | Resolved |
| 13  | <a href="#">2009542</a> | Microsoft PKI Services: Improper Disclosure of CRLs – IDP – New CAs                                         | January 10, 2026   | February 16, 2026 | Resolved |
| 14  | <a href="#">2009543</a> | Microsoft PKI Services: Improper Disclosure of CRLs – Does Not Match CA Subject                             | January 10, 2026   | February 9, 2026  | Resolved |
| 15  | <a href="#">2009545</a> | Microsoft PKI Services: Improper Disclosure of CRLs – Protocol Scheme                                       | January 10, 2026   | February 11, 2026 | Resolved |
| 16  | <a href="#">2021175</a> | Microsoft PKI Services: Failure to update action item status within 3 days                                  | March 5, 2026      | April 3, 2026     | Resolved |
| 17  | <a href="#">2026452</a> | Microsoft PKI Services: Failure to publish Full Incident Report for Bugzilla 2021175 within 14 days         | March 26, 2026     | April 22, 2026    | Resolved |
| 18  | <a href="#">2026453</a> | Microsoft PKI Services: Failure to report Bugzilla 2026452 within 72 hrs                                    | March 26, 2026     | April 22, 2026    | Resolved |
| 19  | <a href="#">2034251</a> | Microsoft PKI Services: Failure to Update Full Incident Report within 14 days of discovering new root cause | April 23, 2026     | May 13, 2026      | Resolved |

Microsoft Public Key Infrastructure Services  
July 28, 2026

## ATTACHMENT A

### LIST OF IN SCOPE CAs

| Root CAs         |                                                                            |
|------------------|----------------------------------------------------------------------------|
| 1.               | AP Root Certificate Authority 2014                                         |
| 2.               | Azure Hardware Root Certificate Authority 2019                             |
| 3.               | Azure Sphere Root Certificate Authority 2020                               |
| 4.               | Microsoft Android Platform Root CA 2021                                    |
| 5.               | Microsoft Code Verification Root                                           |
| 6.               | Microsoft Corporation Third Party Marketplace Root                         |
| 7.               | Microsoft Development Root Certificate Authority 2014                      |
| 8.               | Microsoft ECC Development Root Certificate Authority 2018                  |
| 9.               | Microsoft ECC Devices Root CA 2023                                         |
| 10.              | Microsoft ECC Devices Root Certificate Authority 2017                      |
| 11.              | Microsoft ECC Services Root CA 2021                                        |
| 12.              | Microsoft ESRP Root Certificate Authority 2017                             |
| 13.              | Microsoft Mariner RSA Root CA 2023                                         |
| 14.              | Microsoft Mobile Root Certificate Authority 2015                           |
| 15.              | Microsoft Overlake Root Certificate Authority 2019                         |
| 16.              | Microsoft RSA Devices Root CA 2021                                         |
| 17.              | Microsoft RSA Devices Root CA 2023                                         |
| 18.              | Microsoft RSA Services Root CA 2021                                        |
| 19.              | Microsoft Services Federal Root 1                                          |
| 20.              | Microsoft Services Partner Root                                            |
| 21.              | Microsoft Supply Chain ECC Root CA 2022                                    |
| 22.              | Microsoft Supply Chain RSA Root CA 2022                                    |
| 23.              | Microsoft Surface Device Authentication Root CA 2014                       |
| 24.              | Microsoft TPM Root Certificate Authority 2014                              |
| 25.              | Microsoft Enterprise Identity Verification Root Certificate Authority 2020 |
| Intermediate CAs |                                                                            |
| 26.              | Azure RSA PS CA EOC CA 01                                                  |
| 27.              | Azure RSA PS CA EOC CA 02                                                  |
| 28.              | Azure RSA PS CS AOC CA 01                                                  |
| 29.              | Azure RSA PS CS AOC CA 02                                                  |
| 30.              | Azure RSA PS CS EOC CA 01                                                  |
| 31.              | Azure RSA PS CS EOC CA 02                                                  |
| 32.              | Azure RSA Public Services Code Signing PCA                                 |
| 33.              | Azure Services Linux Kmod PCA                                              |
| 34.              | ESRP0 RSA PCA 2017                                                         |
| 35.              | ESRP2 RSA PCA 2017                                                         |
| 36.              | IDNA SK PCA                                                                |
| 37.              | J2ME Manufacturer Domain CA 2015                                           |
| 38.              | J2ME Trusted Third Party Domain CA 2015                                    |
| 39.              | Linux Boot Loader Signing CA 2016                                          |
| 40.              | Lumia Labeling CA                                                          |
| 41.              | M365 RSA Services Code Signing PCA                                         |
| 42.              | Mariner Trusted Base RSA Code Signing CA                                   |
| 43.              | Microsoft Android Code Transparency and Upload PCA                         |
| 44.              | Microsoft Android Play App PCA                                             |
| 45.              | Microsoft Andromeda Attestation CA 2017                                    |
| 46.              | Microsoft Andromeda Attestation PCA 2017                                   |
| 47.              | Microsoft Andromeda Firmware Debug CA 2017                                 |
| 48.              | Microsoft Atlas Attestation CA 2020                                        |
| 49.              | Microsoft Atlas Attestation PCA 2020                                       |
| 50.              | Microsoft Atlas Firmware Debug CA 2020                                     |
| 51.              | Microsoft Band Firmware CA 2015                                            |
| 52.              | Microsoft Band Firmware Debug CA 2016                                      |

53. Microsoft Benham Attestation CA
54. Microsoft Benham Attestation PCA
55. Microsoft Cerberus AOC CA 01
56. Microsoft Cerberus AOC CA 02
57. Microsoft Cerberus EOC CA 01
58. Microsoft Cerberus EOC CA 02
59. Microsoft Cloud Server AOC CA 01
60. Microsoft Cloud Server AOC CA 02
61. Microsoft Cloud Server EOC CA 01
62. Microsoft Cloud Server EOC CA 02
63. Microsoft Corporation KEK 2K CA 2023
64. Microsoft Corporation KEK 3K CA 2023
65. Microsoft Corporation KEK 4K CA 2023
66. Microsoft Corporation KEK CA 2011
67. Microsoft Corporation Third Party Marketplace PCA
68. Microsoft Corporation UEFI CA 2011
69. Microsoft Corsica AOC CA 01
70. Microsoft Corsica AOC CA 02
71. Microsoft Corsica EOC CA 01
72. Microsoft Corsica EOC CA 02
73. Microsoft Development PCA 2014
74. Microsoft Devices OEM Code Sign CA 2018
75. Microsoft Devices UEFI CA 2016
76. Microsoft ECC Development PCA 2018
77. Microsoft ECC LFF Platform Attestation CA
78. Microsoft ECC LFF Platform Attestation PCA
79. Microsoft ECC NFF Platform Attestation CA
80. Microsoft ECC NFF Platform Attestation PCA
81. Microsoft ECC Surface Accessory Firmware CA 2018
82. Microsoft ECC Surface Accessory Firmware CA 2023
83. Microsoft ECC Third Party PCA 2019
84. Microsoft HoloLens Attestation CA 2018
85. Microsoft HoloLens Attestation PCA 2018
86. Microsoft HoloLens Firmware Debug CA 2018
87. Microsoft IDNA RSA Policy Signing CA
88. Microsoft IoT Hardware AOC CA 01
89. Microsoft IoT Hardware AOC CA 02
90. Microsoft IoT Hardware EOC CA 01
91. Microsoft IoT Hardware EOC CA 02
92. Microsoft Mobile Development PCA 2014
93. Microsoft Mobile PCA 2015
94. Microsoft OEM Custom CA 2014
95. Microsoft Option ROM UEFI CA 2023
96. Microsoft Overlake Agent Signing PCA 2019
97. Microsoft Overlake Celestial Peak AOC CA 01
98. Microsoft Overlake Celestial Peak AOC CA 02
99. Microsoft Overlake Celestial Peak EOC CA 01
100. Microsoft Overlake Celestial Peak EOC CA 02
101. Microsoft Overlake OS Signing PCA 2019
102. Microsoft Overlake Policy Signing PCA 2020
103. Microsoft Overlake STOS Signing PCA 2020
104. Microsoft Pinewood Attestation CA 2019
105. Microsoft Pinewood Attestation PCA 2019
106. Microsoft RSA Third Party PCA 2023
107. Microsoft SCD Claimants RSA CA
108. Microsoft SCD Products RSA CA
109. Microsoft SCD Systems RSA CA
110. Microsoft Secure Launch ECC PCA 2017

111. Microsoft Services Federal PCA 1  
112. Microsoft SH2 Firmware CA 2018  
113. Microsoft SH2 Firmware Debug CA 2018  
114. Microsoft Surface Accessories Windows Firmware CA 2013  
115. Microsoft Surface AFF Firmware CA 2021  
116. Microsoft Surface AFF Firmware Debug CA 2021  
117. Microsoft Surface AFF UEFI PK CA 2021  
118. Microsoft Surface Common Services CA 2014  
119. Microsoft Surface FFF Firmware CA 2018  
120. Microsoft Surface FFF Firmware Debug CA 2018  
121. Microsoft Surface for RT Firmware CA 2012  
122. Microsoft Surface for Windows 8 Pro Firmware CA 2012  
123. Microsoft Surface for Windows RT CA 2012  
124. Microsoft Surface for Windows RT EK Issuing CA 01  
125. Microsoft Surface for Windows RT EK Issuing CA 02  
126. Microsoft Surface for Windows RT EK Issuing CA 03  
127. Microsoft Surface for Windows RT EK Issuing CA 04  
128. Microsoft Surface Ganymede Attestation CA 2017  
129. Microsoft Surface Ganymede Attestation PCA 2017  
130. Microsoft Surface Hub Firmware CA 2015  
131. Microsoft Surface Hub UEFI PK CA 2015  
132. Microsoft Surface LFF 3 Firmware CA 2016  
133. Microsoft Surface LFF 3 Firmware Debug CA 2016  
134. Microsoft Surface LFF 3 UEFI PK CA 2016  
135. Microsoft Surface LFF Firmware CA 2021  
136. Microsoft Surface LFF Firmware Debug CA 2021  
137. Microsoft Surface LFF UEFI PK CA 2021  
138. Microsoft Surface MoBB-1 Boot Core CA 2019  
139. Microsoft Surface MoBB-1 CA 2014  
140. Microsoft Surface NFF Firmware CA 2015  
141. Microsoft Surface NFF Firmware CA 2021  
142. Microsoft Surface NFF Firmware Debug CA 2015  
143. Microsoft Surface NFF Firmware Debug CA 2021  
144. Microsoft Surface NFF UEFI PK CA 2015  
145. Microsoft Surface NFF UEFI PK CA 2021  
146. Microsoft Surface Services for Windows 8 Pro CA 2012  
147. Microsoft Surface Services for Windows RT CA 2012  
148. Microsoft Surface SFF Attestation CA 2013  
149. Microsoft Surface SFF Firmware CA 2013  
150. Microsoft Surface SFF Platform Key CA 2013  
151. Microsoft Surface SH2 Firmware CA 2022  
152. Microsoft Surface SH2 Firmware Debug CA 2022  
153. Microsoft Surface SH2 UEFI PK CA 2022  
154. Microsoft Surface Silicon Partner PCA 2018  
155. Microsoft Surface Stamps CA 2024  
156. Microsoft Surface with Windows RT v2 Boot ROM Fuse CA 2013  
157. Microsoft Surface with Windows RT v2 Firmware CA 2013  
158. Microsoft Surface with Windows RT v2 Platform Key CA 2013  
159. Microsoft Surface with Windows RT v2 Services Mobile CA 2013  
160. Microsoft Surface XLFF 2 Firmware CA 2016  
161. Microsoft Surface XLFF 2 Firmware Debug CA 2016  
162. Microsoft Surface XLFF 2 UEFI PK CA 2016  
163. Microsoft Surface XLFF Firmware CA 2021  
164. Microsoft Surface XLFF Firmware Debug CA 2021  
165. Microsoft Surface XLFF UEFI PK CA 2021  
166. Microsoft Surface XSFF Firmware CA 2018  
167. Microsoft Surface XSFF Firmware Debug CA 2018  
168. Microsoft Surface XSFF UEFI PK CA 2018

169. Microsoft UEFI CA 2023  
170. Microsoft Universal Store OnePay PCA 2015  
171. Microsoft VSMC PCA 2017  
172. Microsoft Windows Group Edition KEK CA 2015  
173. Microsoft Windows IoT KEK CA 2015  
174. Microsoft Windows IoT PCA 2015  
175. Microsoft Windows UEFI PK CA 2017  
176. Microsoft XCloud PCA 2018  
177. MR0 RSA PCA 2022  
178. MR1 RSA PCA 2022  
179. Phones UEFI CA 2016  
180. Surface Factory CA 2018  
181. Windows Hello 11B0C61D CA 2021  
182. Windows Hello 1767C8B4 CA 2018  
183. Windows Hello 19B92965 CA 2018  
184. Windows Hello 2096ADCC CA 2021  
185. Windows Hello 41738710 CA 2021  
186. Windows Hello 5CF190F8 CA 2018  
187. Windows Hello 73CA926A CA 2021  
188. Windows Hello 7BB5EEFC CA 2018  
189. Windows Hello 9F10CB1F CA 2021  
190. Windows Hello B5A8CEAC CA 2018  
191. Windows Hello FPR-I-256 CA 2023  
192. Windows Hello GD-256 CA 2023  
193. Windows Hello Secure Devices PCA 2018  
194. Windows Phone KEK CA 2012  
195. Microsoft Enterprise Identity Verification Code Signing PCA 2020  
196. Microsoft Enterprise Identity Verification WSCV PCA 2020  
197. Microsoft SCD Claimants ECC CA  
198. Microsoft SCD Products ECC CA  
199. Microsoft SCD Systems ECC CA  
200. Microsoft Enterprise ID Verification CS EOC CA 02  
201. Microsoft Enterprise ID Verification CS EOC CA 03  
202. Microsoft Enterprise ID Verification CS EOC CA 01  
203. Microsoft Enterprise ID Verification CS AOC CA 02  
204. Microsoft Enterprise ID Verification CS AOC CA 01  
205. Microsoft Enterprise ID Verification CS AOC CA 03  
206. Microsoft Enterprise ID Verification WSCV AOC CA 02  
207. Microsoft Enterprise ID Verification WSCV AOC CA 03  
208. Microsoft Enterprise ID Verification WSCV AOC CA 01  
209. Microsoft Enterprise ID Verification WSCV EOC CA 02  
210. Microsoft Enterprise ID Verification WSCV EOC CA 01  
211. Microsoft Enterprise ID Verification WSCV EOC CA 03

**ATTACHMENT B**

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

| <b>CP Name</b>                                            | <b>Version</b> | <b>Date</b>    |
|-----------------------------------------------------------|----------------|----------------|
| <a href="#">Microsoft PKI Services Certificate Policy</a> | 3.2.0          | April 20, 2026 |
| <a href="#">Microsoft PKI Services Certificate Policy</a> | 3.1.9          | April 21, 2025 |

| <b>CPS Name</b>                                                                   | <b>Version</b> | <b>Date</b>    |
|-----------------------------------------------------------------------------------|----------------|----------------|
| <a href="#">Microsoft PKI Services Corporate Certification Practice Statement</a> | 3.2.0          | April 20, 2026 |
| <a href="#">Microsoft PKI Services Corporate Certification Practice Statement</a> | 3.1.9          | April 21, 2025 |

**ATTACHMENT C**

**LIST OF MS PKI SERVICES' LOCATIONS IN-SCOPE**

| <b>#</b> | <b>Location Name</b>                     | <b>Location Type</b>                                  | <b>Location</b>          | <b>In-Scope for Physical and Environmental Control Testing</b> |
|----------|------------------------------------------|-------------------------------------------------------|--------------------------|----------------------------------------------------------------|
| 1        | Corporate headquarters and office spaces | Main office                                           | United States of America | No                                                             |
| 2        | Online CA hosting 1                      | Datacenter 1                                          | United States of America | Yes                                                            |
| 3        | Online CA hosting 2                      | Datacenter 2                                          | Ireland                  | Yes                                                            |
| 4        | Offline CA hosting 1                     | Primary offline CA facility                           | United States of America | Yes                                                            |
| 5        | Offline CA hosting 2                     | Disaster recovery / secondary offline CA facility     | United States of America | Yes                                                            |
| 6        | Secure storage 1                         | Secure storage for online CAs and offline CAs         | United States of America | Yes                                                            |
| 7        | Secure storage 2                         | Cold storage for online and offline CAs               | United States of America | Yes                                                            |
| 8        | Secure storage 3                         | Disaster recovery / secondary storage for offline CAs | United States of America | Yes                                                            |
| 9        | Secure storage 4                         | Third-party cold storage for offline CAs              | United States of America | Yes                                                            |
| 10       | Secure storage 5                         | Secure storage for online CAs and offline CAs         | Ireland                  | Yes                                                            |