

The Slandala Company
203 North Lee Street
Falls Church, Virginia, 22046
703 851 6813
jimmy.jung@slandala.com



12 September 2025

Caroline Godfrey
Chief Security Officer
WidePoint Cybersecurity Solutions Corporation
11250 Waples Mill Road
South Tower, Suite 210
Fairfax, VA 22030

The Slandala Company conducted a compliance audit of the WidePoint Cybersecurity Solutions Corporation Public Key Infrastructure (PKI) to verify that the PKI was operating in accordance with the security practices and procedures described in the following Practices and Policies:

- *WidePoint Non-Federal Issuer Shared Service Provider Certification Practice Statement [WP-NC-NFISSP-CPS], Version 3.5, June 12, 2024*
- *WidePoint Non-Federal Issuer Shared Service Provider Certificate Policy [WP-NC-NFISSP-CP], Version 3.7, July 7, 2025*
- *XTec Non-Federal Public Key Infrastructure X.509 Certificate Practices Statement for Interaction with WidePoint, Version 1.7, 30 October 2023*

WidePoint operates several Public Key Infrastructure systems collectively referred to as the Information Assurance/Identity Management System (IA/IDM), including the following certificate authorities:

- CN=WidePoint NFI Root 2, OU=Certification Authorities, O=WidePoint, C=US
- CN=WidePoint ORC NFI 4, OU=Certification Authorities, O=WidePoint, C=US
- CN=WidePoint NFI CA 5, O=ORC PKI, C=US
- CN=WidePoint NFI CA 6, O=ORC PKI, C=US
- CN=Senate PIV-I CA 6, O=ORC PKI, C=US

The Compliance Audit evaluated the Certificate Authority, Directory Server, Certificate Status Servers and Card Management Systems components associated with these CAs. The compliance audit reviewed findings from the previous year. There have been no major changes to the system.

The XTec NFI Issuing CA (NFI 4) is operated by XTec staff. CA operations of the XTec NFI Issuing CA are included in this audit report. RA Audits for systems issuing from the XTec CA are managed by XTec.

The audit also evaluated conformance to the requirements of the Memorandum of Agreement (MOA) between the WidePoint (NFI) PKI and the FPKIPA covering interoperability between the WidePoint NFI PKI and the FPKI, signed June 2023.

The compliance audit was performed via interviews, documentation reviews and site visits performed in May and June 2024. This audit covers the following period:

- Audit Period Start: May 2024
- Audit Period Finish: August 2025

The operational compliance audit was performed using a requirements decomposition methodology and was initiated by first performing a direct CP-to-CPS traceability analysis.

The WidePoint Non-Federal Issuer Shared Service Provider Certification Practice Statement was evaluated for conformance to the WidePoint Non-Federal Issuer Shared Service Provider Certificate Policy

CPS practices found to not comply or address the requirements of the applicable policies, as part of the traceability analysis are categorized as “Disparate.”

The CPS was reviewed and decomposed into requirements, and the requirements were then evaluated to determine the general methodology for their evaluation and the activities that should be taken by the auditor to fulfill the audit of that requirement. The audit step activities are performed during the site visits and documentation reviews. Observations and recommendations are identified and may be included. Findings and data are recorded during these activities, and are categorized as follows:

- Complies – operations comply with the practices documented in the CPS,
- Discrepancy – operations do not comply with the practices documented in the CPS,
- Recommendation - operations comply with the practices documented in the CPS; however, improvements to the implementation could be considered.

The audit was performed by Mr. James Jung of The Slandala Company, who acted as the lead auditor. Mr. Jung has performed audits of PKI systems since 2002 and has more than 35 years’ experience in the design, implementation and certification of information assurance systems. He is certified by the International Information Systems Security Certification Consortium (ISC) ² as a Certified Information Systems Security Professional (CISSP) and is certified by the Information Systems Audit and Control Association (ISACA) as Certified Information Systems Auditor (CISA). He has implemented or operated PKI systems for the Department of State, the Department of Energy, the Federal Bureau of Investigation, the Department of Homeland Security, the United States Patent and Trademark Office (USPTO) and other agencies and commercial companies. He has provided PKI audit and compliance support for the Department of State, the Department of Labor and several of the Department of Defense (DoD) agency Registration Authorities, Local Registration Authorities and External Certificate Authorities. Mr. Jung has been the lead auditor for the Department of Defense Certification Authorities the Department of Treasury Public Key Infrastructure (PKI) and Shared Service Provider (SSP) and the Federal PKI (FPKI) Trust Infrastructure, including the Federal PKI Common Policy Framework (FCPF) Certification Authority and the Federal Bridge Certification Authority (FBCA).

Mr. Jung has not held an operational role or a trusted role on the WidePoint PKI systems, nor has he had any responsibility for writing the Certificate Practices Statements. The Slandala Company and Mr. Jung are independent of the WidePoint PKI and its operations and management.

Information from the following documents was used as part of the compliance audit.

- *WidePoint Non-Federal Issuer Shared Service Provider Certification Practice Statement [WP-NC-NFISSP-CPS], Version 3.5, June 12, 2024*

- *WidePoint Non-Federal Issuer Shared Service Provider Certificate Policy [WP-NC-NFISSP-CP], Version 3.7, July 7, 2025*
- *XTec Non-Federal Public Key Infrastructure X.509 Certificate Practices Statement for Interaction with WidePoint, Version 1.7, 30 October 2023*
- *Memorandum of Agreement between The United States Federal Public Key Infrastructure Policy Authority (“Policy Authority”) and WidePoint Cybersecurity Solutions Corporation [Non-Federal Issuer, signed June 2023*
- *Agreement between XTEC, Inc. and WidePoint Cybersecurity Solutions Corporation to define the identity management services, Effective Date: 11/01/2018*
- *Authority to Operate (ATO) – USAGM’s Office of Security’s (SEC) Credentialing Services, October 20, 2022*
- *(SEC) Credentialing Services XTEC Inc. (XTEC) Business Continuity Plan (BCP) for the AuthentX Identity and Access Management System and Credential Management System (IDMS / CMS), Version 0.4, 2021*
- *FEDRAMP Privacy Impact Assessment (PIA) XTEC, Inc AuthentX Cloud, Version 1.5, February 2021*
- *AuthentX Cloud Configuration Management Plan 1.5, January 26, 2021*
- *AuthentX Cloud Roles & Responsibilities Version 5.1, 25 March, 2024*
- *FIPS 201 / FICAM Evaluation Program Remote PIV-I Card Annual Testing Report Version 1.1 WidePoint ORC NFI 4 (PKI Shared Service Provider) & US Courts (Issuing Organization), June 18, 2025*
- *FIPS 201 / FICAM Evaluation Program Remote PIV-I Card Annual Testing Report Version 1.1 WidePoint ORC NFI 4 (PKI Shared Service Provider) & U.S. Agency for Global Media (Issuing Organization), June 20, 2025*
- *FIPS 201 / FICAM Evaluation Program Remote PIV-I Card Annual Testing Report Version 1.1 WidePoint ORC NFI 4 (PKI Shared Service Provider) & Fiserv/Citibank (Issuing Organization), May 8, 2025*
- *FIPS 201 / FICAM Evaluation Program Remote PIV-I Card Annual Testing Report Version 1.1 WidePoint ORC NFI 4 (PKI Shared Service Provider) & Federal Reserve Bank (Issuing Organization), May 29, 2025*
- *FIPS 201 / FICAM Evaluation Program Remote PIV-I Card Annual Testing Report Version 1.1 WidePoint ORC NFI 4 (PKI Shared Service Provider) & National Science Foundation (Issuing Organization), June 6, 2025*
- *PIV-I CMS Operational Guide (AFS), Rev:20250106*
- *Information Assurance/ ID Management Local Registration Authority (LRA) Appointment Letter Template*
- *WidePoint Information Assurance/ Identity Management (IA/IDM) Procedure # 4-6.1, Information Assurance/Identity Management Disaster Recovery Site Safe Procedure, approved 4/5/2016*
- *WidePoint Information Assurance/ Identity Management (IA/IDM) Procedure # 4-5, Information Assurance/Identity Management System Backup Procedure, approved 4/5/2016*
- *WidePoint Information Assurance/ Identity Management (IA/IDM) Procedure # 7-0, Information Assurance/Identity Management Disaster Recovery (DR) Site Access, approved 4/5/2016*
- *WidePoint Rules of Behavior*
- *Information Assurance/Identity Management Privacy Policies and Procedures Policy*
- *WidePoint Information Assurance/Identity Management (IA/IDM) System Risk Management Plan, April 5, 2016, Version 1.4*
- *WidePoint Trusted Role List - November 19, 2021*
- *WidePoint All Programs Contingency Plan [WP-NC-Cont-Plan], Version 3.7, January 17, 2024*

- *WidePoint Information Assurance / Identity Management (IA/IDM) Contingency Plan Test Report, 23 February 2024*
- *Audit Report Number of Records Analyzed by Day of Audit Report Samples*
- *WidePoint PKI Archive List*
- *WidePoint Incident Report Tracking Form – WP-NC-Inc-Rep INCIDENT TRACKING ID: 2024-12-03_WP-NC-Inc-Rep*
- *Trusted Role List (WidePoint Authorized Roles / First Responder Team Designation), December 31, 2024*

The WidePoint Non-Federal Issuer (NFI) Certificate Practices Statement was evaluated for conformance to the Operational Research Consultants, Inc. Non-Federal Issuer Certificate Policy.

The analysis identified one instance where policy description and the practice description were disparate.

The XTEC Non-Federal Public Key Infrastructure X.509 Certificate Practices Statement for Interaction with WidePoint was evaluated for conformance to the Operational Research Consultants, Inc. Non-Federal Issuer Certificate Policy.

The analysis identified twenty-one instances where policy description and the practice description were disparate.

The audit included a compliance audit of the practices described in the WidePoint NFI CPS. Eight items did not comply with the policy or practice statements,

The audit included a compliance audit of the practices described in the XTEC NFI CPS. Three items did not comply with the policy or practice statements,

RA audits are conducted by sampling the RA pool and rotating through the available RAs each year.

RA operations were audited at the following sites:

Accenture Federal Services in Washington, DC

Audit for RA operations under the XTEC CA were assessed separately and reports for those audits were reviewed. Two missing criteria were identified.

No failures were found that suggested that the system had been compromised or operated in an overtly insecure manner. It is the lead auditor's opinion that the WidePoint PKI systems provided reasonable security control practices.

X

James Jung
Lead Auditor