National Cyber Security Centre
a part of GCHQ

NCSC CYBER RESILIENCE TESTING (CRT)

Product Assessment Report:

FIOR

November 2026

Version 1.0

OFFICIAL

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

National Cyber Security Centre
a part of GCHQ

Document Details	
Client	FIOR
Product	AI Gateway v26.2
Country of Manufacture	UK
Title	Cyber Resilience Testing Assurance Statement
Author	Eva Warren
CRTF	NCC Group, XYZ Building 2 Hardman Boulevard, Spinningfields, Manchester, M3 3AQ
Version	1.0
Date	09 November 2026
Document Ref	CRT Assurance Statement No. 01/01
Status	Final Assessment

Report Revision History		
Version	**Date**	**Summary of changes**
0.1	22/10/2026	Initial draft
0.2	26/10/2026	Updated report following additional evidence provided by FIOR
0.3	09/11/2026	Updated report following internal QA review
1.0	09/11/2026	Definitive Issue

Disclaimer - Please note that this report only covers the specified product version(s), so later updates would need re-assessment to fully understand the changes and any associated risks.

OFFICIAL

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

National Cyber Security Centre
a part of GCHQ

1. Product Details

Scope Definition

FIOR AI Gateway is a software appliance that operates at the network boundary, serving as an intelligent security gateway for AI agents and automated workloads. It verifies identity, evaluates trust and enforces security policies in real time, ensuring every agent request is authenticated, authorised and compliant before permitting access to enterprise systems or executing actions.

Key Functions

The key functions of the FIOR product:

Key Function	Specification
Per-Agent PQC Identity	Unique ML-DSA-65 X.509 cert per agent, bound to TPM 2.0 / Secure Enclave PCR values.
Surgical Revocation	OCSP-stapled revocation broadcast to every gateway in the fleet.
Behavioural Attestation	Every agent action Merkle-chained and signed with ML-DSA-65.
ABAC Policy Engine	45+ configurable constraints embedded in cert: rate, scope, time, network.
Offline Verification	Delta CRL distribution for air-gapped / edge deployments.
Human vs Agent Proof	Signed subject_type X.509 extension + PCR / biometric divergence.

Specifications

Feature	Specification
Communication Protocols	HTTPS, TLS 1.2, TLS 1.3, mTLS
User Authentication	Supabase Auth / GoTrue, bcrypt, TOTP MFA
Security Features	X.509 certificates, SPIFFE identities, Ed25519, ML-DSA-65 where enabled for AI-agent identity verification; AES-256-GCM; SHA-256; HSTS, PostgreSQL Row-level-security
Network Connectivity	Outbound HTTPS between the customer-deployed Gateway and the FIOR control plane; no internet-facing inbound Gateway listener is required; the Gateway uses the customer's network controls, and the FIOR-hosted control plane operates within a VPC.

OFFICIAL

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

National Cyber Security Centre
a part of GCHQ

2. Summary of Product Performance

P1.1: Follow an established secure development framework	**P1.2: Assess risks from the ingestion of third-party components**	**P1.3: Have a clear process for testing software before distribution.**
P1.4: Follow 'secure by design' throughout the development lifecycle	**P2.1: Protect the build environment against unauthorised access.**	**P2.2: Control and log changes to the build environment**
P3.1: Distribute software securely	**P3.2: Implement an effective vulnerability disclosure process.**	**P3.3: Have processes to detect, prioritise and manage vulnerabilities**
P3.4: Report vulnerabilities to relevant parties where appropriate	**P3.5: Provide timely security updates, patches and notifications**	**P4.1: Specify the level of support and maintenance provided**
P4.2: Provide at least 1 year's notice to customers of when the software will no longer be supported	**P4.3: Make information available to customers about notable incidents**	**P5.1: Design the product to be usable**
P5.2: Ensure only authorised users have access to product data and functionality	**P5.3: Protect sensitive data and the integrity of the product**	**P5.4: Enable the logging and monitoring of security events**

Key:	All claims met		Assumptions		Risks		Risks & Assumptions	

OFFICIAL

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

National Cyber Security Centre
a part of GCHQ

3. Identified Risks for the Principles

3.1 Risks

Principle	Doubt(s)/Unmet Claim(s)	Risks	Impacts
P5.1	5.1.1.1.1.2 - Accessibility testing demonstrates the design supports disabled people in securely installing, using and maintaining the product	There is a risk that some of the products security features may not operate as intended because people are not fully supported in using the product securely.	Complete all accessibility tests to meet WCAG compliance.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

National Cyber Security Centre
a part of GCHQ

4. Claims Analysis

4.1 Claims Not Met

Principle	Claim	Reason Claim Unmet
NONE	NONE	NONE

4.2 Claims With Doubts

Principle	Claim	Reason for Doubt
P5.1	5.1.1.1.1.2 - Accessibility testing demonstrates the design supports disabled people in securely installing, using and maintaining the product	There is a risk that some of the products security features may not operate as intended for disabled people as they are not fully supported in accessing the product.

4.3 Assumptions

Principle	Claim	Reason for Assumption
NONE	NONE	NONE

OFFICIAL

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

National Cyber Security Centre
a part of GCHQ

5. Claims Amendments

5.1 Claims Removed

Principle	Claim	Reason Claim Removed
NONE	NONE	NONE

5.2 Claims Amended

Principle	Claim	Reason for Change
NONE	NONE	NONE

5.3 Claims Added

Principle	Claim	Reason for the Addition
NONE	NONE	NONE

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

National Cyber Security Centre
a part of GCHQ

6. The CRT Testing Process

Cyber resilience testing is a principles-based assurance (PBA) approach from NCSC. The aim of a CRT assessment is to gain an understanding of a product's security posture and any high-level risks. This is formed by gathering and analysing evidence, based on a standardised set of criteria related to product development, design and management. The output of the assessment is intended to support potential customers of a product in making informed risk-based decisions about a product.

The CRT process is based on a hierarchical set of 'Principles' and 'Claims'. There are a series of Claims that sit within each Principle. The vendor of a product must provide evidence to explain how its product meets the relevant security criteria in the Claims.

6.1 Assessment Criteria

Indicator	Description
Fully Met Claim	A claim for which there are no Doubts. This means all aspects of the claim have been evidenced.
Assumption	A claim that is knowingly not evidenced. There are three main types of assumptions: a. A claim that is out of scope of the CRT assessment. In most cases this will be an assumption that the product is deployed or used in a certain way. b. A claim that is not evidenced as it is assumed it is not relevant to the product's intended application. c. A claim that is not evidenced because a design decision has knowingly assumed that any resulting risk will be readily accepted by users.
Doubt	Where not all aspects of a claim have sufficient evidence or the evidence is not fully convincing, then there will be a Doubt against that claim.
Unmet Claim	A claim that evidence has demonstrated to have not been met.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©