PRESS RELEASE

FIOR
The Enforcement Layer for AI

Monday 16 November 2027 GMT 1300

FIOR AI Gateway Achieves NCSC CRTF Cyber Resilience Assessed Status

Independent assessment conducted by an NCSC-assured Cyber Resilience Test Facility (CRTF), using a methodology approved by the NCSC

LONDON, 16th November : FIOR, the identity and enforcement layer for AI, today announced that its AI Gateway is now NCSC Cyber Resilience Assessed.

Fior has completed a Cyber Resilience Testing (CRT) assessment conducted by NCC Group. The assessment was carried out under the National Cyber Security Centre's (NCSC) Principle Based Assurance (PBA) scheme.

NCC Group is assured by the NCSC to carry out Cyber Resilience Testing, which assesses how well a product can protect itself against common cyber-attacks when connected to the internet. The assessment of FIOR covered FIOR AI Gateway and assessed the product against 18 NCSC principles across five themes: secure design and development; build environment security; secure deployment and maintenance; communication with customers; and product-specific usage, design and operation. The assessment recorded that none of the 72 security claims made by FIOR were unmet claims.

As agents begin to act across enterprise applications, APIs, data and infrastructure, security teams need to know which agent is acting, who authorised it and whether each action falls within policy, before that action is executed. This result gives government and enterprise buyers a third-party reference point at a time when organisations are facing increased cyber risk from AI-assisted attacks, just as they move AI agents out of pilots and into live systems.

FIOR's AI Gateway acts as an independent self-sovereign identity and enforcement layer for AI agents using patent-pending deterministic identity technology. It gives each agent a cryptographically secure identity, determines what that agent is authorised to do and enforces those permissions deterministically at runtime, with rapid revocation and tamper-evident audit records. All of the processes are carried out inside the enterprise boundary by the

FIOR software. No information leaves the enterprise and no data needs to be sent to an identity provider.

David Williams, Founder and CEO of FIOR, said:

> *"Many companies have told us that they cannot exploit the benefits of AI until they are confident that the controls governing those agents are based on an identity that is secure.*
>
> *We have already made our first commercial customer deployments. But we chose to put our AI Gateway through NCSC CRTF Cyber Reslience Assessment to help potential customers to gain confidence. Completing the process with no unmet claims gives our government and enterprise customers an objective basis for their decisions.*
>
> *We are grateful to NCSC who have been far sighted in offering this new program which, whilst exhaustive and detailed we were able to complete in under six months. The UK is becoming a World leader in the assurance of AI models and security.*
>
> *The bedrock of FIOR's enforcement layer software for agents and tools is unique patent-pending deterministic identity technology that is bound to hardware, cryptographically secure and entirely self-sovereign with no third-party dependencies.*
>
> *Achievement of CRTF Cyber Reslience Assessed status delivers further uniqueness to the FIOR AI Gateway product since I believe FIOR is the first AI identity and enforcement platform in the World to publicly complete such an assessment."*

The NCSC CRT Product Assessment Report for FIOR AI Gateway is available on the FIOR website and the full report is available to customers.

ENDS

NOTES TO EDITORS

About Cyber Resilience Testing

Cyber Resilience Testing (CRT) is the NCSC's assurance methodology for evaluating how resilient a connected product is to cyber-attack. Assessments are carried out by independent test facilities assured by the NCSC, known as Cyber Resilience Test Facilities (CRTFs), and are grounded in the NCSC's Principle Based Assurance approach, which looks at risk outcomes rather than compliance with a fixed checklist. A CRTF assessment is not a certification. Results apply only to the

product version assessed, and an assessment report is not an endorsement of a product.

Products that complete a CRTF assessment may be described as “NCSC CRTF – Cyber Resilience Assessed”. Assessment conducted via an NCSC Cyber Resilience Test Facility (CRTF) does not imply compliance with regulatory standards, best practice, or any other form of certification.

About FIOR

FIOR is the identity and enforcement layer for AI.

FIOR’s AI Agent Enforcement Gateway enables organisations to identify AI agents, determine what each agent is authorised to do and enforce those permissions before actions are executed.

Designed to operate across organisational and technology boundaries, FIOR provides deterministic, cryptographically secure and hardware bound identity that is unique to every agent. This bedrock of identity is used to enforce policies, make rapid revocation and deliver tamper-evident audit capabilities for autonomous AI systems and tools. The FIOR AI Gateway platform is entirely self-sovereign. No data about the existence or activities of AI agents is required to leave the enterprise boundary in order to gain an identity, and the product works in offline, air gapped environments.

FIOR works with enterprises, governments, technology companies and infrastructure providers internationally seeking to deploy AI agents securely and at scale.

www.fior.group

Media contacts

Henry Lerwill and Francesca Eaton

Hawthorn Advisors | fior@hawthornadvisors.com