Rethinking Authentication

Readers' workflows are changing. No longer are they reliably connected to their institution's network when accessing resources. IP recognition-based legacy approaches can require complex workarounds to cope with mobile workflows.

Older systems can also pose a significant security risk. IP addresses are open to various methods of abuse, and the lack of transparency makes accurate usage reporting difficult.

OpenAthens provides a SAML-based approach to single sign-on that is more secure, reliable, and transparent than IP recognition.
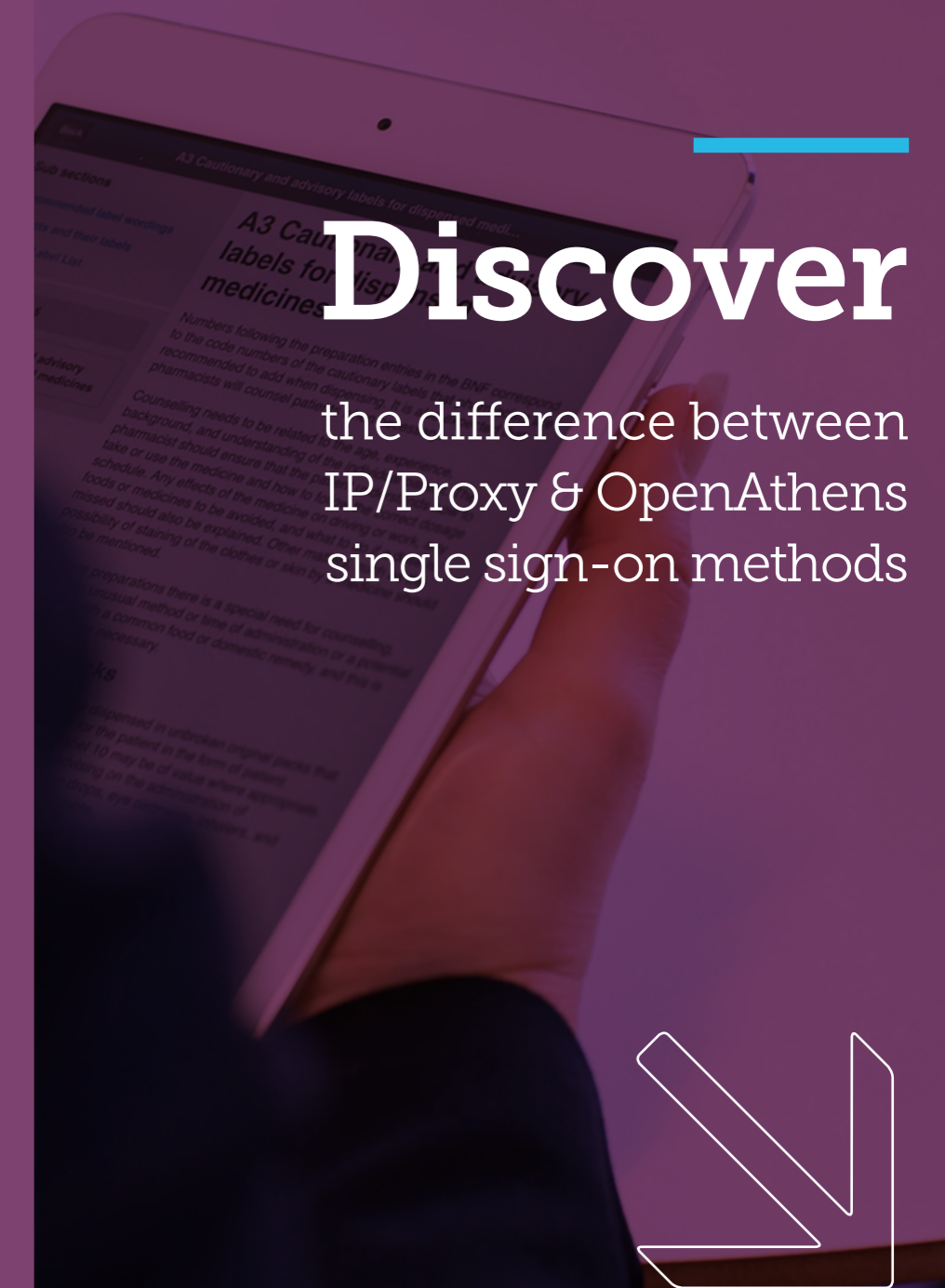
- **Security**
  SAML-based authentication limits exposure to attackers

- **Trust**
  Readers and resources protected from fraud and misuse associated with IP recognition

- **Simplicity**
  Full SaaS/cloud solution – no in-house development resource required

- **Transparency**
  Statistics reporting provides insight at the institutional, departmental, and individual login level

Glossary of terms

- **Identity Provider (IdP)**
  An organization or product that confirms user identities and attributes to enable them to access content owned by service providers. Examples of IdP products are OpenAthens, Shibboleth and Ping Federate.

- **IP Address**
  A numerical reference (e.g. 123.123.123.0) that identifies the location of a device on a network or the wider internet, managed globally.

- **IP Recognition**
  A form of access management that grants access to resources based on the IP address of a user's device.

- **OpenAthens**
  An access management system for organizations or content providers (IdPs or SPs in SAML terms) that facilitates SSO access to subscription content.

- **Proxy Service**
  Software that acts as an intermediary between users and content. Often used to facilitate remote access to subscription-based content.

- **Remote Access**
  Allows users to access library holdings (particularly subscription content) with their normal login credentials when they are outside of the institution network (for example, at home or using a mobile device).

- **SAML**
  Security Assertion Markup Language. A protocol for exchanging security information between identity providers and service providers.

- **Service Provider (SP)**
  An organization that provides content or services.

- **SSO**
  Single Sign-on. Providing users with access to many different systems through a single set of login details.

Discover
the difference between IP/Proxy & OpenAthens single sign-on methods

T: **+44 (0) 1225 437 514**
E: **openathens@eduserv.org.uk**
W: **www.openathens.org**

Single Sign-on Journeys Compared

Authentication should provide assurance to readers, institutions, and publishers that connections are trustworthy. Legacy methods focus on recognition – based on network location – rather than true authentication of readers' credentials, which OpenAthens provides.

○ Included ○ Optional	OpenAthens	IP/Proxy
Cloud hosted solution	●	○
Administration interface	●	
Group-level security (permission sets)	●	
Customisable end-user access portal	●	
SSO solution	●	○
SSO with IP recognition	○	○
Integration with local applications	●	○
REST based API	●	
Service Desk support	●	○
Requires local IdM infrastructure	○	○
Supports any attribute set	●	
Create user categories	●	
Ability to connect directly to LDAP	●	○
Add own branding to user interface	●	○
Out-of-the-box statistics reporting	●	
Out-of-the-box statistics by user category	●	
Out-of-the-box statistics by individual user	●	
Export report data	●	○
SSO with Federated resources	●	
SAML 1x capability to log into resources	●	
SAML 2x capability to log into resources	●	
Define which attributes are sent to each Service Provider	●	
Resource link generator & knowledgebase (Redirector)	●	

OpenAthens' approach to authentication provides the flexibility to adapt to changing workflows, the security to protect against fraud and misuse, and the transparency librarians need to make informed purchasing decisions.

Visit **www.openathens.org** today for more information.

OpenAthens
Authentication

VS

IP/Proxy
Recognition

Simple set up – complete SaaS

Technical set up – in-house development

SAML Handshake

Secure – End User / Publisher / Library

160 9920 46

488 1176 33

883 2237 00

463 9814 15

811 4367 32

Two Way Transparency / Individual Stats

IP Recognition

Insecure / Open To Spoofing

Proxy Server

? Anonymous Users

No Individual Details / Anonymous

Publisher

Publisher

Global Standard In Authentication

Simplicity for the library

Legacy Technology / Work Around

Complexity for the library