SPS Secure Mobile for Public Safety
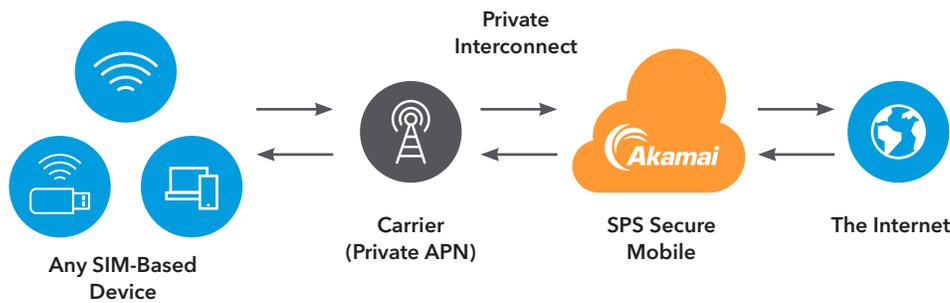
Secure Mobility for First Responders

Public safety agencies (PSAs) are becoming increasingly mobile, which is driving the need for a coordinated strategy that involves protecting employees, data, and devices from cyberattacks and for compliance purposes. IT administrators face the challenge of securing data across multiple devices and networks at the federal, state, and local levels.

SPS Secure Mobile

SPS Secure Mobile provides first responders with a safer internet experience on smartphones, ruggedized tablets, and cellular routers. IT administrators can facilitate highly secure access to sensitive content over cellular and Wi-Fi networks, with additional capabilities to monitor all traffic and any alerts and notifications required.

Because of its vantage position in the carrier's core network, SPS Secure Mobile provides strong protection against cyberattacks, such as malware, phishing, and ransomware, before they happen. SPS Secure Mobile is the first line of defense for protecting sensitive information used by PSAs.

Benefits

- Keeps sensitive personal information away from malicious actors

- Protects all types of SIM-enabled devices including cellular routers and MiFis

- Applies robust usage policies consistently across the entire mobile estate

- Delivers tangible benefits from day one, removing complexity from mobile deployments

Technical Architecture

Any SIM-Based Device → Carrier (Private APN) → Private Interconnect → SPS Secure Mobile (Akamai) → The Internet

Key Features

Network Security and Compliance
Stop malware and malicious content before it gets to devices. Block unknown or unregistered domains that could be used for DNS hijacking or redirection attacks. SPS Secure Mobile is a central part of a regulatory compliance strategy.

Advanced Reporting and Analytics
Provide essential data to enable fast decision-making and protect valuable mobile data and devices. SPS Secure Mobile provides insights to determine the main drivers of data usage and the effectiveness of usage policies.

Content Filtering
Manage access to 165 categories of websites that cover more than 1 billion domains. Deny video streaming services such as Netflix and YouTube. Confirm devices are used for business purposes only.

Data Controls
Customize the internet experience of individuals and groups. Limit internet access speeds and set mobile data caps at the individual or group level. Support compliance with personal data regulations, such as SOX, HIPAA, or GDPR.

Compliance
We take protecting data seriously. We have implemented the strictest industry security best practices, including FIPS 140-2, CJIS, and ISO 27001, to ensure our services are built to meet the most rigorous standards.

FIPS 140-2 Compliance　　　**CJIS Compliance**　　　**ISO 27001**

Akamai Security and Personalization Services are designed to help organizations become digitally secure and connected wherever they are. SPS Secure Mobile is a mobility service that delivers a secure internet experience on all SIM-enabled devices. The service can be deployed without the need for cumbersome equipment or VPNs. Devices can be enrolled with minimum effort and disruption to users, and start delivering benefits from day one.

Source:

1. Mobile Security Index 2020

People at Risk

77%
of public sector organizations said that a mobile security compromise would put people's lives at risk and 90% said that their employees' data is as sensitive as the people they serve.[1]

To learn more, click here or talk to your account manager.