Government of Canada API Standards: Ensuring Interoperability and Security

The Government of Canada's Digital Standards outlines how APIs should be developed across the Government of Canada (GC) better to support integrated digital processes across departments and agencies. [1] These standards emphasize the following key principles:

- RESTful Architecture: APIs must follow the RESTful model by default, representing resources as URLs and using JSON.
- Clear Message Schemas: Message schemas should be easy to understand and consume, leveraging industry-recognized common information models.
- Security First: Security must be at the forefront, with practices such as enforcing secure communications and protecting access to APIs.
- Interoperability: Consistent metadata and encoding, using Unicode for encoding and ISO 8601 for datetime format, ensure interoperability.
- Lifecycle Management: APIs should be evolved and supported throughout their lifecycle, with a clearly defined Service Level Agreement (SLA).
- Performance and Throttling: API performance should be benchmarked periodically, and throttling mechanisms should be implemented to control throughput against the stated SLA.

Key Regulatory Updates:

- Québec's new incident reporting rules for financial firms (effective 2025) mandate swift reporting of security breaches to the Autorité des marchés financiers (AMF).
- OSFI is increasing its focus on financial institutions' operational and API security resilience, requiring reassessment of compliance measures.
- Bill C-27, if passed, will introduce significantly increased fines for data breaches, emphasizing the importance of robust API security.

Why It Matters: Adherence to the Government of Canada's API standards ensures consistency, interoperability, and security across government digital services. These standards promote efficient data exchange between departments and with the public, improving service delivery and enhancing the citizen experience. Moreover, organizations need to adjust to changing regulations to prevent penalties and uphold public trust, particularly regarding the management of sensitive data.

API Security Requirements:

- **Secure Communications:** Enforce secure communication protocols like TLS for all API interactions.
- **Access Controls:** Employ robust authentication and authorization methods to secure API endpoints. The growing regulatory focus on data protection and incident reporting makes these requirements even more critical.

How Salt Security Helps: Salt Security focuses on API security while aligning with standards. Its API discovery feature offers visibility crucial for managing and securing APIs. Posture governance aids lifecycle management by spotting vulnerabilities affecting performance or security, and threat protection upholds a "Security First" principle. The ability to monitor data in motion through APIs provides insights into data exchanges within the Canadian government. Additionally, Salt Security helps organizations meet Québec's new reporting requirements and comply with OSFI's heightened security expectations. Its strong threat detection and data visibility also help mitigate risks of penalties under Bill C-27. Learn more about API Security and Compliance in our **White-paper.**