Client Use Case

Public Sector

Securing sovereign cross-border data flows without disrupting critical operations

How Certes Secures Public Sector Data Systems

A major public sector organization operates highly sensitive systems that enable secure, real-time data exchange across multiple sovereign jurisdictions. Supporting critical international operations, the environment depends on continuous availability, strict regulatory compliance, and absolute control over how sensitive data moves between interconnected systems, third-party networks, and national boundaries.

Overview

Large public sector bodies operate some of the most critical digital infrastructure in the world These systems enable real-time sharing of highly sensitive identity and security-related data which are foundational to support operations across continents. This environment demands continuous availability, strict compliance with regional data protection laws, and absolute control over how sensitive data moves between jurisdictions.

For more than 14 years, Certes has supported such a mission by protecting nearly 55 petabytes of sensitive data in motion across a distributed, pan-region infrastructure.

> "Public sector organizations operate highly sensitive, distributed environments where data must move securely across sovereign boundaries without disrupting operations. The challenge is no longer just defending networks, but ensuring that even if systems are compromised, the data itself remains protected, controlled, and compliant at all times. This deployment shows how a data-centric approach can deliver that protection at continental scale."
>
> **- Simon Pamplin, Chief Technology Officer, Certes**

The Challenge

Sovereignty, Scale, and Zero Margin for Error

The public sector body faced a uniquely complex challenge:

- Sensitive data moving continuously across sovereign national boundaries
- 24/7 operational systems
- Strict legal frameworks governing data access, privacy, and control
- Hundreds of interconnected systems distributed across multiple sovereign jurisdictions.

In this environment, traditional network security creates exposure. Once attackers gain access, data moving between systems can be intercepted, manipulated, or exfiltrated, which would trigger regulatory consequences and erode trust between nations. The customer needed to guarantee that:

- Operational performance and availability were never compromised
- Security controls were consistently enforced across a fragmented infrastructure
- Data remained protected and compliant with regional regulations as it moved across borders
- Sovereign control was maintained across all countries

Failure would not be contained to a single organization. It would impact multiple nations, disrupt cooperation, and undermine public trust at a continental level.

The Solution

Data Protection Embedded Into Every Cross-Border Flow

Certes deployed its Data Protection & Risk Mitigation (DPRM) capabilities across the customer's distributed infrastructure, applying protection directly to data in motion.

This ensured that sensitive data remained unreadable and unusable, regardless of where it travelled or who accessed the network.

Key elements of the deployment include:

- Protection enforced across hundreds of devices distributed, multi-national infrastructure
- Continuous protection of data flows between critical government systems
- Centralized policy control with local enforcement, preserving national sovereignty
- Over 56 million cryptographic key rotations executed to maintain data integrity and control
- Daily key rotation policies applied across high-value data exchanges
- No disruption to existing infrastructure, enabling deployment without rearchitecting systems

By embedding protection into the data itself, the public sector body achieved consistent security enforcement across all participating nations without requiring disruptive infrastructure changes.

The Outcome

Continental-Scale Resilience and Continuous Compliance

The results demonstrate sustained, large-scale protection across one of the most sensitive environments in the world:

- **55PB** Nearly 55 petabytes of sensitive data protected in motion
- Secure data exchanges
- 14+ years of continuous, uninterrupted operation
- Full alignment with regional data protection and security requirements
- Protection maintained with no impact to performance or availability
- **56m** Over 56 million key rotations ensuring ongoing data control

This approach enables the customer to maintain secure, real-time collaboration between nations while ensuring that sensitive data cannot be exploited, even if systems are accessed or networks are compromised.

For public sector systems where trust, sovereignty, and security are critical, protecting the data itself ensures that operational integrity is maintained under all conditions.

CERTES

Any App.
Any Infrastructure.
Anywhere.

info@certes.ai
certes.ai
300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108