

# Provide secure, individualized government services

In a connected world, where integrated voice, video, and data can be aggregated in unique ways and delivered to many devices, personalized and highly secure access to confidential information has become an absolute priority for government organizations. Therefore, a streamlined way of assigning and managing identity, authentication, and access rights is now a cornerstone requirement in a 'people-ready' organization.

Today, government organizations are evolving their service delivery model away from basic Web sites serving up information from stovepipe ministry-specific applications, and starting to deploy smarter, more personalized, self-service solutions for staff and citizens alike.

Consequently, they face two security imperatives. Firstly, they need to ensure that access to data is secure by providing identity information for employees, external contractors, and business people who work with government. Secondly, they need to manage access and identity for citizens wanting to access payment services, social services, immigration, public safety, travel, and other government information.

To assist governments in providing comprehensive identity management, Microsoft solutions range from eAuthentication and single sign-on for secure staff network access, right through to eID log-in for business partners and citizens. Microsoft technologies also streamline the provisioning and retirement of identities, as well as reporting, audits, and lost password/PIN resets.

Microsoft® Active Directory® makes it simple to manage, migrate, and assign the network identities and relationships that operate across networked environments. These identities can then be leveraged by core applications including email, collaboration, and digital rights management to provide users with transparent authentication. Security credentials can also be shared or translated through federation services.

Complementing this, Microsoft® Identity Integration Server automates identity updates across disparate platforms while maintaining the integrity and ownership of data across the organization. This synchronization of identity information enables governments to provide users with single sign-on, vastly simplifying access to all of the networked applications and services they are authorized to use.

Sophisticated authentication solutions such as smart cards with digital certificates can increase management overhead. To avoid this, Microsoft® Certificate Lifecycle Manager, turnkey deployment and policy-driven workflow provide a solution which helps simplify security management for the network administrator and end user, with tools that automate common management functions and enable users to self-administer common tasks.

By deploying the Microsoft® platform, government organizations can help address increasing privacy compliance requirements, such as Sarbanes-Oxley and HIPAA. These include: providing a single security credential across many services, delivering consistent sign-on and single sign-on, identity mapping, initial user identification, initial user provisioning, and user and enrollment management. For citizens, Windows CardSpace™ provides a consistent user experience which helps to protect against tampering and spoofing.



"By utilizing our existing Windows environment and Active Directory, the Server and Domain Isolation solution enabled us to meet security compliance effectively with no additional hardware or software costs."

Kazuya Kawatani, IT Promotion Section,  
Information Technology Promotion  
Department, City of Sapporo, Japan

Are your **people**  **ready?**

# Featured Microsoft solution

## Provide secure, consistent, personalized access to information and services

A new government employee arrives at Human Resources (HR) for the first day at work. HR requests a range of routine documentation for the new employee, then enters the required information into the eHR system, and sends the employee to physical security.

Using Microsoft® Identity Integration Server the new employee's identity is propagated through to physical security and the IT helpdesk, streamlining the initialization process. Staff at Physical Security issue an RFID-enabled smart card with a photo ID. The RFID code is associated with the buildings that the new employee is authorized to access, and is automatically added to the physical access control system.

Staff in IT Services can automatically provision the employee with a network login and email account. The network account leverages Microsoft® Active Directory® to provide single sign-on access to the line-of-business

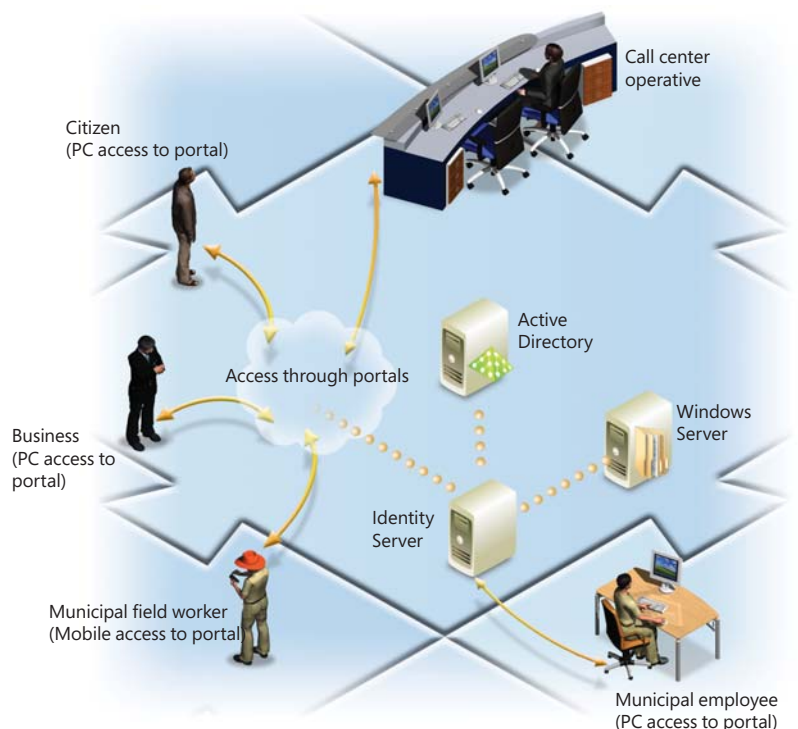
applications and collaboration resources the new employee will need.

The new employee accesses the office using the RFID-enabled card, logs in to a workstation and attempts to access a line-of-business application. Even though the network login has been propagated to the application, the appropriate certificates and

authorizations have not been established. However, using a self-service forms-based workflow, the new employee requests the smart card-based certificates and authorization from the manager. Upon receipt, the employee installs the smart card to generate the appropriate certificate for authorized access to the application.

### Relevant Microsoft technologies

- Windows Server®
- Microsoft® Active Directory®
- Microsoft® Identity Integration Server
- Microsoft® Certificate Lifecycle Manager



## Microsoft and our solutions partners can help your organization provide secure identity management

Microsoft Certified Partners are independent companies that can provide you with the highest levels of technical expertise, strategic thinking, and hands-on skills. In terms of identity and access management, for example, they can help your government organization to:

- Automate identity and access management across your organization so that employees and citizens alike can benefit from simple, secure access to government information, systems, and services
- Seamlessly integrate new technologies, for example, smart cards and digital certificates, to deploy flexible service options for citizens, enabling them to make applications and obtain other services either online, via PDA, or using the phone
- Create a 'one-stop shop' for government services across multiple departments, vastly simplifying citizen interactions
- Improve operational efficiency with consistent, centralized identity lifecycle processes, streamlined federation systems, and simplified management
- Simplify compliance and help minimize risk with auditable processes for access rights
- Reduce helpdesk costs by providing people with tools to manage routine tasks, such as changing passwords or resetting smart card PINs
- Get a single view of employee and citizen activities and use this intelligence to improve citizen services, increase operational efficiency, and improve security
- Boost interagency collaboration with comprehensive security, identity, and authentication services making it easy to share information across organizational boundaries
- Protect citizen privacy and organizational data with customized identity and access management solutions

# Microsoft solution helps municipal government achieve security compliance

In 2004, the local government of the Japanese City of Sapporo established a security policy to define and control how the city maintained its information assets and identity management. With 12,000 staff working in 870 departments, the city needed to comply with a new security policy to ensure that its information assets were not vulnerable to external and internal security attacks.

## Situation

The City of Sapporo is the fifth largest city in Japan, with a population of approximately 1.9 million. The city intranet contains sensitive and confidential information about the city and its citizens. With the deployment of highly connected networks and the growth of online information assets, the local government of Sapporo faced new security issues. The challenge was to provide employees with even greater access to information, but at the same time increase network security through a robust identity management solution.

## End-to-end authenticated communications

The first step towards providing a secure identity management solution came with the introduction of a Server and Domain Isolation solution based on Windows® Internet Protocol Security (IPsec) and Microsoft® Active Directory®.

This enabled policy-driven logical network isolation, end-to-end authenticated communications, virtually tamper-proof data integrity and data confidentiality, all without the city having to upgrade hardware and software or retrain its staff.

All communications between domain-managed computers and servers are now authenticated using IPsec, as determined by the Group Policy in Microsoft Active Directory. This helps to prevent employees or rogue users from gaining unauthorized access to internal servers containing sensitive data.

Microsoft Active Directory provides a single sign-on capability and a central repository for information for the entire infrastructure of the organization, vastly simplifying user and computer management and providing better access to networked resources.

**“By utilizing our existing Windows environment and Active Directory, the Server and Domain Isolation solution enabled us to meet security compliance effectively with no additional hardware or software costs.”**

*Mr Kazuya Kawatani, IT Promotion Section  
Information Technology Promotion Department,  
City of Sapporo, Japan*

## Improved security

As part of a layered defense approach, Server and Domain Isolation complements other host and network-based security technologies used by the city to enable greater resiliency in the presence of intranet network security threats. These include antivirus, anti-spyware, firewalls, and intrusion detection systems.

By dynamically segmenting their Windows® environment into more secure and isolated logical networks based on policy, the City of Sapporo has helped further strengthen security by creating an additional layer of protection that can be easily maintained and updated.

## Better for business, better for Sapporo

City of Sapporo IT managers are now confident that critical network communications are authenticated and occur only between known, managed computers connecting to their network, satisfying compliance requirements.

Windows IPsec and Active Directory-based solutions help make information easily available to employees and citizens, without sacrificing security.

[www.microsoft.com/casestudies/casestudy.aspx?casestudyid=4000000161](http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=4000000161)

**Overview:** The local government City of Sapporo, Japan, provides services for more than 1.9 million citizens, and employs over 12,000 people working in 870 departments.

## Business Situation

When the local government of the City of Sapporo provided their employees with access to networked files, they needed to comply with a new security policy to ensure that information assets were not vulnerable to external and internal security attacks.

## Solution

The City of Sapporo deployed Server and Domain Isolation based on Windows® Internet Protocol Security (IPsec), and Microsoft® Active Directory®.

## Benefits

- Improved security and compliance
- Ability to assign authorization to individuals, groups, and entire departments
- Protection of confidential data
- Compatibility with existing systems
- Enhanced value of IT and reduced management costs

## Partner(s): Microsoft

### Software & Services:

- Windows® Internet Protocol Security (IPsec)
- Microsoft® Active Directory®
- Microsoft® Operations Manager
- Windows Server®
- Windows® XP

[www.microsoft.com/csp](http://www.microsoft.com/csp)

© 2008 Microsoft Corporation. All rights reserved. Microsoft, the Microsoft logo, Active Directory, Windows, Windows CardSpace and Windows Server are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. 11192e-1207/MS

Part No. 098-109028

**Microsoft®**