Flemish Government provides seamless access for citizens

Supported by IBM Business Partner SecurIT

Overview

The need
Provide citizens and employees with simple, secure and fast digital access to available Flemish Authorities resources, now and in the future.

The solution
IBM Premier Business Partner, SecurIT, designed and implemented an integrated software solution for the Flemish Authorities, combining its TrustBuilder software with IBM Security solutions.

The benefit
Reduces the time and cost to introduce new applications significantly; allows tremendous savings through the sharing of one centralized platform for many government institutions; provides six million citizens with seamless access to government services.

Combining IBM security access management software with SecurIT TrustBuilder provides citizens and employees with simple, secure and fast digital access to all available Flemish Authorities resources, now and in the future.

The Flemish Government controls Flanders, which is the northern federated state of Belgium, with Brussels as its capital and about six million inhabitants. Its legislative and executive powers include broad and exclusive domestic and international responsibilities. The powers of the Flemish Government and the Belgian federal government do not overlap. This allows Flanders to control its own departments and policies on economics, foreign trade, health care, energy distribution, housing, agriculture and horticulture, environment, public works and transport, employment policy, culture and education, science and societal innovation.

The need
Citizens of Flanders have digital access to the services that can be provided to them by more than 100 government sites, administrated by the departments listed earlier. The central service platform allowed for shared Access Control Management (ACM) across the sites. However, the old ACM platform lacked important capabilities to fulfill the future vision of the Flemish Authorities, such as suppleness for changes and the introduction of new internal and external applications, flexibility in how citizens prove their identities, and ability to grant access based on user role or capacity at a particular point in time.
The vision
In replacing ACM with what is now called ACM3, the Flemish Authorities had three specific goals to support the fulfillment of its future vision and platform strategy:

1. **Secure**: The ACM3 environment must provide secure access to applications where users are strongly identified by different means, such as the Belgian Electronic Identity card (eID).

2. **Simple**: The use of the ACM3 environment for accessing applications must not introduce a level of complexity that can discourage a user (including citizens) from using the published applications.

3. **Fast**: The ACM3 environment should offer generic building blocks which can be reused to allow fast and easy integration of applications with the ACM environment, and allow the replacement or upgrade of specific parts of the environment as needed, with minimum or no impact on the other components.

The solution
ACM3 now has a new infrastructure based on a service-oriented architecture (SOA) that addresses the need for upgrades with minimum impact on the other components (see diagram below).

---

“**The new infrastructure will provide citizens and employees with simple, secure and fast digital access to all available government resources, now and in the future.**”

—Wim Martens, Strategy Manager, Flemish Government
SecurIT, an IBM Premier Business Partner, designed and implemented an integrated software solution for the Flemish Authorities, combining its TrustBuilder software with IBM Security Access Manager and IBM Federated Identity Manager software.

Access enforcement and single-sign-on is handled by IBM Security Access Manager software with TrustBuilder providing support for simultaneous use of multiple authentication methods (username and password, eID card, federal token, Flemish Authorities token, and so on), depending on the security policy desired and user preferences.

The Virtual Identity layer is provided by a combination of IBM Security Access Manager software, IBM Federated Identity Manager software, and TrustBuilder, the latter to allow interaction with the user on capacity and authentication method selection, and access to the internal user repositories, including retrieval of authentication and authorization attributes.

The Virtual Identity Provider is responsible for redirecting identification and authentication requests to the proper internal or external Identity Provider in accordance with the required level of authentication and the user's capacity for the session. All communications between layers of this model are based on the Security Assertion Markup Language (SAML) 2.0 standard.

A Central Logging building block based on IBM Security Information and Event Manager software is responsible for centralizing and consolidating log information regarding administrator and end-user activity on the ACM3 environment. This also serves as the search console in case of incidents to easily find incident related events or troubleshoot the environment.

**The results**

**Secure Context-aware identification of users and applications**

In the real world, a person has only one identity but can act under multiple titles or “roles”, such as “citizen”, “public servant”, “notary” and so on. In the digital world, the distinction of role is also required when a
user consults an application to help ensure the access to information and capabilities is appropriate to the role that a user is working in. This means that the ACM3 environment is able to identify users and their roles when they use an application available via the ACM3 platform.

**Multiple authentication possibilities and step-up**
The ACM3 environment is now able to offer multiple authentication mechanisms to the users. This provides the user with great flexibility in a very secure manner. Existing and common authentication mechanisms are supported such as the electronic ID card, the federal token and the Flemish Authorities token, but other Authentication mechanisms can easily be integrated into the ACM3 environment to help ensure compatibility and flexibility with future evolutions, such as cloud and mobile services. When a higher level of identity assurance is required for accessing a more restricted application, step-up authentication is possible.

**Incoming and outgoing federation**
The ACM3 platform has a Virtual Identity Provider building block that creates the Flemish Authorities Identity Provider to allow external parties to authenticate at the Flemish Authorities. It is also capable of routing a user authentication to other specific Identity Providers, which allows the ACM3 platform to provide authentication of users as a service. This authentication service can be provided internally or externally by a third party. This means that the Flemish Authorities could act as an authentication service for external parties or partners.

**Simple**
**Simple operations management**
The ACM3 platform has simple operational management allowing the administrator to easily make changes to the environment, publish new applications or search log files.

Configurations and rules can be managed centrally. For example, the policies applicable for one URL may be needed by several components or sites but can be managed in a single location. All activity (both by administrators and by end-users) are being logged time-synchronously as to allow the establishment of a formal audit trail that helps confirm the completeness and integrity of data and the tracking of these events.
Fast
Service-oriented architecture
ACM3 has an infrastructure based on a service-oriented architecture that addresses the need for upgrades with minimum impact on the other components.

Benefits to all
The new ACM3 platform offers a substantial value to the Flemish Authorities:

- It reduces the time and cost to introduce new applications significantly, a substantial benefit in a rapidly changing landscape with several government sectors launching new initiatives to leverage the Internet and reach out to the citizens.
- The sharing of one centralized platform for many government institutions allows tremendous savings on capital and operational expenses, contributing to the cost savings all governments are seeking.
- The platform provides six million citizens with seamless access to all Authorities’ services with context-aware digital identities using multiple authentication means, offering a level of freedom to people to choose the appropriate method of identification for each individual in accordance with centrally defined security policies.

ACM3 is also a major step forward for the Flemish Authorities in preparing for the digital world of tomorrow. It provides seamless interaction between multiple domains and can easily cope with a fast changing environment for user identification, both within the government’s realm and with upcoming cloud and mobile prospects.

For more information
To learn more about IBM Security solutions, please contact your IBM sales representative or IBM Business Partner, or visit the following website: ibm.com/security

To increase the business value of your IBM Security solutions, participate in an online community. Join the IBM security community at: http://instituteforadvancedsecurity.com

For more information about SecurIT, visit: www.securit.biz