Security
Technology

Digital Identity
Centralised Management of Security Mechanisms

Authors: **Dr. Chandima Costa, Dr. Harald Ritter**
Version: **1.0**

Abstract:
In order to access different systems within a company, employees often have to use different access codes. By using a unique, digitally stored employee ID for all systems, the corresponding administration processes are extensively harmonised. This results in significant cost saving potentials, providing advantages for the company and for its employees as well. In addition, the company's security is improved. The following document describes the basic technology and gives an overview on possible applications and benefits.

NOVOSEC
Aktiengesellschaft

Sulzbacher Straße 29-39
65824 Schwalbach am Taunus, Germany
Phone +49 (0)6196/88289-0
Fax +49 (0)6196/88289-11
contact@novosec.com, www.novosec.com

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus
Telefon 06196/88289-0, Telefax 06196/88289-11
contact@novosec.com, www.novosec.com

Dream or Reality?

Monday, 9:00 a.m.: Employee M. reaches his desk and connects his notebook into the network. He reads his emails, takes some orders and prints reports to be prepared for the meeting at 10:00 a.m. Once logged in and authenticated there is no need for bothersome further inputs of user accounts for different applications; no loss of time, no forgotten passwords. Times are gone where someone needed an account for each single application which had to be requested from different administrators that, by accident, were currently not available due to admin training!

Monday, 10:00 a.m.: Meeting. The beamer is connected. Presenting Powerpoint slides, interrupted by performing some internet research. Finally a glance on the sales statistics of last week! The team is automatically entitled to view its own sales performance in detail as well as the sales totals of the other teams stored on a company server.

Monday, 11:00 a.m.: The new colleague arrives. Her best welcome: she gets only one access account. With this she can access all applications and data she is entitled for. It was pretty easy to organise this: one email, signed by her supervisor. No routing slip, no signatures, no walks and waiting. So everyone is looking forward to meet the new colleague, and she is happy as well.

Monday, 12:30 p.m.: Lunch break. The desktop PCs are left totally secured. No chance for unauthorised persons to get access to the network!

Monday, 2:00 p.m.: Visiting a customer. During the conversation M. easily logs into the company network to get information and type in the order. The access is managed via VPN; the order is authenticated and assigned to M. The connection is encrypted and therefore secure. The transaction is binding, traceable and auditable.

Monday, 6:00 p.m.: Employee M. is already on his way home. The order from 2:00 p.m. has a respectable volume and therefore needs a confirmation from his supervisor. The supervisor gets the order automatically, signs it digitally and is not only happy about this nice order but also about the efficient workflow. No tray, no signature books, no search for documents and penholders!

Monday, 6:15 p.m.: The supervisor goes home and wonders about the reduction of working hours.

This dream could be reality in your company already today! Standardised administration, centralised user management, Single Sign-On, hierarchical entitlement model, increased access security – all possible with a digital employee ID.

How can this employee ID be designed? Is a chip card required? Is a general password enough? How complex is the required infrastructure? There is no general answer. But there are basic techniques available for each digital employee ID as well as standard processes for managing them.

Basic Technologies

The basic technologies that need to be provided with every digital employee ID are mechanisms for encryption and authentication.

Encryption

The most common instruments for electronic communication are email and World Wide Web. More and more company internal data are exchanged via email or stored on servers. Very often these data are

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus
Telefon 06196/88289-0, Telefax 06196/88289-11
contact@novosec.com, www.novosec.com

confidential. Encryption prevents that unauthorised persons can read them.

Authentication
An authentication proves that a person (or a computer, etc.) indeed is what he/it pretends to be. Without authentication and the associated determination of the communication partner's identity a trustworthy electronic communication over open networks is impossible.

Transaction Release
In order to initiate a transaction with an explicit declaration of intent a transaction release is required. This can be done e.g. via an electronic signature.

Electronic Signatures and Certificates
One way of implementing named mechanisms is the use of electronic signatures and certificates. An electronic signature provides authenticity of messages; the use of certificates also allows checking the communication partner's identity. Electronic signatures may be legally binding due to either national laws or contracts.

For example, employee M. uses "Encryption" when typing in the order at the customer's office and sending it to the company. He authenticates himself to the server within the company network when he accesses confidential documents like last week's statistics.

Usage of these technologies may improve procedures within a company and offers a simple, comfortable and therefore efficient way of working. Questions about technical problems like installation, support and usage have to be kept away from the employee. But what is the best way to roll out all these technologies to the staff? How should the required infrastructure and the internal company's workflows look like?

Processes

The following processes are required for the usage of digital employee IDs within a company:

- Creation/management of the digital employee IDs
- Definition/administration of the entitlement model
- Workflow control

Creation/management of the digital employee IDs
The first step towards issuing a digital employee ID consists of collecting the employee data from different local sources within the company (personnel data, access rights, etc.). In addition to this, functionality for revocation and renewal of digital employee IDs is required for their central administration.

Definition/administration of the entitlement model
For every company the entitlement model will be defined in respect of the company's structure and its business processes. Based on this model the access rights are defined and managed for each task and role that may be assigned to an employee. According to these rights the employee's individual access to applications and business processes may be controlled.

Workflow control
In order to control the workflows efficiently during the usage of a digital employee ID, authentication of the employee should be separated from the verification and granting of rights. During authentication the data contained in the digital employee ID are used to determine the employee's identity. After the identification it will be checked whether he has the right to use the desired application based on the pre-defined entitlement model in advance. The data produced or

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus
Telefon 06196/88289-0, Telefax 06196/88289-11
contact@novosec.com, www.novosec.com

exchanged during authentication should be stored to support auditing and reporting.

Applications

One company-wide, unique digital ID per employee may be used for numerous tasks of various characteristics. As examples, some of them are explained in the following.

Access control
Only authorised employees are allowed to use distinct PCs within the company (*access control to desktops and servers*).
In addition, access to applications and data within the company should only be granted to a restricted group (*access control to data via networks*).
An electronic employee ID may also be used to access buildings or single rooms within the company (*personnel access control*).

VPN-access
A virtual private network allows secured access from outside to any required information and business processes, e.g. for sales staff.

Single Sign-On
Single Sign-On means that, after one single authentication, a user has access to all systems, applications and data he is entitled to. No additional action like input of a password is required for the real accesses.

If the digital employee ID is issued as hardware token (e.g. on a chip card), additional possible "mobile" applications arise:
One possible application is the automatic locking of desktop computers when the digital employee ID card is pulled out of the reader. In case the digital employee ID is also used for physical access control, the employee has to carry it whenever he leaves his work place. Therefore it is impossible for intruders to use an unsecured computer in order to gain access to the company network.
Further possible applications are automated time recording (monitoring) e.g. when entering or leaving the office building or at login and logout of desktop computer, as well as cafeteria billing.

Benefits

Introducing a digital employee ID will result in several advantages for both the company and the employees.

Benefits for the company
Separating authentication and transaction release from the application and business logic generates a substantial cost reduction when introducing new applications. Administration, maintenance and support will become easier and more transparent resulting in further cost savings due to central storage of administration data and hierarchically organised maintenance of user rights. Access rights may be granted "on site" (e.g. by the head of project for project data and systems).
Furthermore, the error rate will be reduced and the security will be increased within the company. For example, the potential security risk that employees write down some of the numerous passwords will be eliminated. In case of emergency ("loss" of digital employee ID, retirement of an employee, etc.) all user rights can be revoked with one single action (revocation of employee ID). Due to the possibility of assigning transactions to a unique, company-wide digital ID business workflows will become transparent and auditable.

Benefits for the employees
Employees also gain considerable advantages out of the implementation of a digital employee ID. Ease of use is their main benefit. The memorising of new passwords is obsolete. Carrying numerous cards or

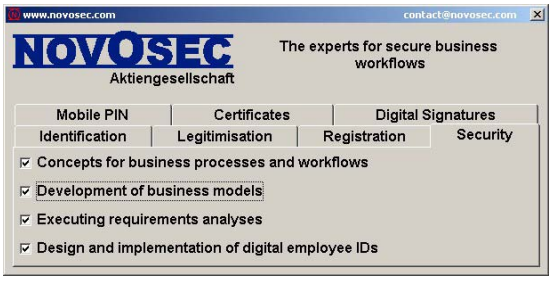
Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus
Telefon 06196/88289-0, Telefax 06196/88289-11
contact@novosec.com, www.novosec.com

identification documents such as access cards for company areas or data centres, cafeteria cards, etc. is no longer necessary. In addition, processing of essential workflows and accessing relevant information may be simplified resulting in more efficient work.

Conclusion

Various possibilities exist for the realisation of digital identity management. The principal task is to choose the best alternative with maximum benefit for the company and best convenience for the employees. To achieve this target, a detailed analysis of the company's prerequisites has to be done. This provides the basis for an optimised implementation of digital identities. Only with a proper implementation, individually designed for the company, the huge benefits of digital identity management for both the company and the employees can be fully achieved.

Are you interested in these topics? Do not hesitate to contact us:
chandima.costa@novosec.com
harald.ritter@novosec.com



Further documents are available at:
http://www.novosec.com/downloads