secmaker

Security and Virtual Desktop Environments

Companies and organizations are more mobile and flexible than ever before. These rapid changes are increasing the pressure on IT departments to more quickly and cost-effectively adapt IT environments to new conditions and needs. Increased flexibility also places new demands on IT security to protect information and applications from unauthorized view and access.

To find competitive solutions, IT managers re-evaluate their organizations from the ground up, often resulting in the virtualization of the IT environment. Virtualization and centralized management of applications and data increases flexibility and lays the foundation for improved IT security. A complete solution also needs to identify and authenticate the end user in a consistent and uniform manner, regardless of where they are located or what terminal they are using. The combination of PKI and smart cards offers a cost-effective and user-friendly alternative for high security in virtual IT environments

Dissolved corporate boundaries raise the security challenge

Today's IT managers are facing greater and more complex challenges than ever before.

Private companies and public organizations are becoming increasingly mobile and flexible. Employees move about extensively, both within the workplace and outside, visiting customers, travelling, or simply working from their desk at home. More than 75% of employees in a typical Scandinavian company are currently estimated to be working on the go.

More and more organizations are also spreading out across diverse geographic locations. Corporate geographic boundaries are dissolving, and organizations become distributed over increasingly larger areas.

Modern companies and organizations are more and more likely to permit consultants, project contractors and telecommuting, which is blurring the lines between internal and external stakeholders.

Information is a key resource, and constant access to information is a prerequisite for an organization's employees to be able to do their work. Today's IT organizations, tasked with supporting flexible businesses and their mobile employees with the right tools, information and applications, are facing all new challenges. The need to make information accessible anytime and anywhere has to contend with high security requirements for internal, classified and business-critical information

"The need to make information accessible anytime and anywhere has to contend with high security requirements for internal, classified and business-critical information."

Different roles – different needs

What makes the situation even more complex is that most businesses consist of several different divisions, often with very diverse responsibilities. Employees in different organizational units have different needs when it comes to mobility and different requirements for support in terms of information and applications. For the sake of simplicity, modern mobile employees can be divided into three categories:

Mobility in the workplace

Employees in the healthcare sector are highly mobile within the workplace itself. There is a great need for healthcare staff to be able to access information, such as medical records and pharmaceutical information, while on the go. It is becoming increasingly common for work sessions to be transferred from one terminal to another as healthcare workers move between different departments or buildings during their high-pressure workdays. Meanwhile, information concerning a patient's medical

conditions, medication and treatment is of a sensitive nature. It is therefore important that the IT environment enables flexibility, without the slightest compromise to patient security or confidentiality.

Many employees in the retail sector work under similar conditions: with a high degree of mobility within a confined area. When retail personnel move through the store or warehouse, they need continual access to various applications such as POS systems, product databases and price lists to make sure they can provide excellent customer service. Sharing POS systems requires fast user switching with retained security. Information is usually of a less sensitive nature in retail than in healthcare, but the requirements for conformance and financial monitoring linked to individual bonus systems require flexible and reliable solutions.

Total mobility

While healthcare and retail workers move within a confined area, sales reps, field service personnel and senior management often move within an even larger professional sphere, working from customer or partner offices, hotels, airports and even restaurants.

The information and the services that the mobile employees need to access can include anything from Microsoft Office to CRM applications, systems for handling work orders, pricing systems, financial monitoring systems, and so on. Many of the services require direct connection to central, internal corporate business support systems and databases.

Stationary external workplaces

An increasing number of employers are allowing – and expecting – employees like managers, administrators and various types of specialists to work from home. This means that modern mobility solutions must also cover completely external workplaces.

In practice, this often entails data transfer outside company network boundaries, via email correspondence or by being copied onto an unprotected USB memory stick. IT departments typically have limited influence over home office environments. They are now facing the challenge of ensuring that workplaces with other hardware and other applications than the organization's own can still meet the required IT security requirements.

"The rapid changes are increasing the pressure on IT departments to more quickly and cost-effectively adapt IT environments to new conditions and needs."

Flexibility – the IT department's nightmare?

The new challenges for the modern IT department can be summarized in four points:

Increased organizational flexibility

Along with rapid changes in organizations and companies come increased demands for IT to keep up and continuously adapt IT solutions to new conditions. This entails both the rapid and smooth integration of new employees or organizations into the existing IT environment and the ability to cost-effectively add new functionality and new services in order to take advantage of new technologies and business opportunities.

The challenge is often not in identifying or developing new IT tools and applications, but rather in implementing these into the organization and into each individual employee's workplace as quickly and as cost-effectively as possible.

Multiplier effect: user * terminals * applications

The fact that different types of employees work according to different processes and have different needs for IT support increases the complexity of the challenge. The combination of services, applications, information, and a myriad of different terminals such as laptops, desktops, workstations, smartphones and tablets, means that the number of combinations is multiplied almost indefinitely. Moreover, all of these different types of IT work environments can exist in the same organization, expected to be supported by a single IT department.

Provisioning, administering, troubleshooting and upgrading each individual employee's local IT environment, operating system and different types of applications is resource-intensive. Securing an IT environment that meets all the unique needs of each individual could become the IT manager's worst administrative and costly nightmare.

Security requirements for increased mobility

As the company's employees become increasingly mobile, so do business applications and information. Increased accessibility brings increased vulnerability, partly due to the risk that hackers or organized crime could take advantage of the poor security procedures for mobile work, partly due to the risk of mobile phones, laptops or tablets being lost or stolen.

Impaired IT security means business-critical threats and direct costs for the organization. IT and security managers are facing the challenge of protecting classified information and business-critical applications from unauthorized access. The complexity lies in doing this without the security impeding the organization's employees in their mobile work. Usability and security must go hand in hand.

"IT and security managers are facing the challenge of protecting classified information and business-critical applications from unauthorized access. The complexity lies in doing this without the security impeding the organization's employees in their mobile work. Usability and security must go hand in hand."

Demands for cost control and efficiency

For most IT departments, a fourth all-encompassing challenge may be added to the above three: In most places, the unstable economic situation of recent years has led to an increased scrutiny of IT budgets. This means that changed conditions must often be dealt with within existing budget constraints.

Today's IT departments are therefore forced to perform a balancing act to deliver more service and increased flexibility with improved security – for the same money as before.

Virtualized work environment increases control and flexibility

To find competitive solutions to current challenges, many IT managers are electing to re-evaluate their organizations from the ground up. One area that comes under scrutiny in such evaluations is the traditional client-server architecture and its limits. Instead, companies increasingly see a virtualized IT environment as an attractive alternative.

Limitations of the traditional client-server environment

A traditional client-server environment consists of software, operating systems and applications installed on each employee's unique terminals: desktop computers, laptops, notebooks, smartphones and tablets.

Typically, different types of terminals have different types of operating systems and application support, and thereby different conditions. Applications and software services are developed and customized for each unique type of terminal and its operating systems. Organizations with different types of users with separate needs thus have a wide range of combinations and variations that need to be verified, provisioned and administered. This is work that will ultimately become slow, expensive and difficult to manage. The local handling of each individual client when, for example, new software needs to be installed or updated, also impacts the total cost.

"Virtualization makes it possible to centralize the management of applications and data to a data center. This gives IT managers all new opportunities to more efficiently manage and administer the organization's IT environment."

Virtualization – how it works

One of the fundamental principles of client virtualization is to separate the operating system and the applications the user is running from the physical, local hardware. This makes it possible to centralize applications and data to a data center. Instead of local installation for each individual employee computer, all applications and operating systems run concurrently in a central environment. This centralized control gives IT managers

new opportunities for more effectively managing and administering the central, shared image of each operating system or application platform.

The organization's employees gain access to a complete digital desktop environment with selected applications and services from a thin client, a regular computer, smartphone or tablet. Since all services – applications and operating systems – are run centrally, the digital work environment is made available to the end user through streaming.

When the employee's digital workplace is moved from the end user's computer to a centralized data center, the input for provisioning, storing and supporting each individual client is reduced. Since no applications are installed locally, there is less risk of incompatibility between different software versions and thereby also less need for testing. In a virtualized environment, all compatibility issues can thus be handled centrally once and for all.

The separation of applications and operating systems from the physical device also makes it possible to run all applications on all types of terminals without local customization. Regardless of where the end user is located and how they choose to work, the work environment and the user experience are the same.

Virtualization with Citrix XenDesktop and XenClient

XenDesktop and XenClient offer an attractive alternative to desktop virtualization.

Citrix XenClient

Citrix XenClient is a so-called "hypervisor," which enables the virtualization of clients to the organization's employees. This means that multiple virtual operating systems can run side by side on the same physical computer, completely isolated from each other.

This in turn makes it possible to create one private environment and one professional work environment with different operating systems and different applications that work side by side. Since the different operating systems can be completely isolated from each other in terms of security, it is possible to fully protect the company's applications and files, while at the same time the user is free to do whatever they like on their own private virtual computer.

Citrix XenClient also offers the advantage of "checking-out" and running the virtual desktop client offline, locally on the employee's client. This has traditionally not been possible in a virtualized environment.

"Creating one private and one professional work environment that work side by side but are completely isolated from each other protects the company's applications and files, while giving the user full freedom on their own private virtual computer."

Citrix XenDesktop / XenApp

Citrix XenDesktop makes it possible to quickly and securely deliver a complete digital desktop to all users in the organization, whether stationary or mobile. One of the advantages of this solution is that it offers three different alternatives for virtualization and how the virtual desktop can be made available to the end user:

- **A server-hosted desktop** is hosted in a Windows Server, Remote Desktop Service, and shared by several users. Multiple users connect to the same virtual server and share resources in the same operating environment. An entire desktop or a single application can be delivered, with the perception that they are run entirely locally.

- **In desktop streaming,** the virtual desktop is installed and run centrally from the data center. Both the operating system and applications are delivered as a streaming image over the network to the end user, who has the same user experience as with a locally installed service.

- **When using Virtual Desktop Infrastructure** (VDI), an image of the virtual desktop is hosted as its own virtual machine running on a hypervisor in the central data center.

The IT department can thus offer each employee the best experience for them, depending on whether they have access to the network or need to be able to work locally and sync data when the connection becomes available again.

Advantages of virtualization

Reduced costs for IT administration

One of the recognized benefits of a virtualized IT environment is the ability to reduce effort and thereby the operational costs for IT administration and support. Since a virtual desktop environment means that a single image and version of applications and operating systems run centrally for the entire company, there is less pressure on the IT environment to handle different combinations of operating systems, applications and terminals. Since different applications and platforms are isolated from each other and the local system environment, there is also a reduced need to customize and test various services with each other to ensure compatibility.

With fewer installations of each application, the risk that errors will be

multiplied by the number of employees in the organization disappears. Should anything go wrong and an update needs to be backed up, this can be handled once, in one central location.

Finally, centralized handling and administration minimizes the need for IT personnel to visit each individual employee, which also helps contribute to reduced operating costs.

Increased flexibility and shorter Time-To-Market

Thanks to central management, it is often much faster to introduce new versions and upgrades of platforms and applications in a virtual desktop environment than in the traditional client-server environment. A new client can be added in just a couple of minutes, enabling employees to get started with their work immediately. An organization with hundreds or even thousands of employees can upgrade its operating system or application platform within a few hours instead of the weeks or months it used to take.

Through a smoother and more effective introduction of new IT services in the organization, virtualization not only helps lower costs, but also helps provide employees with access to new tools faster than ever before. This increases the potential for improved productivity and quickly taking advantage of new business opportunities.

Reduced equipment and energy costs

Since applications and operating systems are run centrally and then streamed to users, the need for local processing power is reduced. When all the processing power is located centrally, it provides an opportunity for rationalization in terms of both hardware cost and power consumption. When using thin clients, which consume significantly less energy than "fat" ones, the organization will begin to see even further energy savings.

Greater flexibility for users

In a virtual desktop environment, the end user is no longer dependent on a personal or dedicated terminal being available in order for them to perform their job. Employees can access their complete desktop "on-demand", regardless of which machine they use: a PC at the office, a laptop or notebook at home, or a completely external computer at a customer's or partner's office. The user experience remains the same. End user flexibility increases dramatically, giving the end user the opportunity to choose when, where and how to work. Virtualization can thereby also offer the flexibility demanded in dynamic work environments such as hospitals or retail businesses.

"In a virtual desktop, all employees can access their entire desktop "on-demand" no matter what machine they are using: a PC at the office, a laptop or notebook at home, or a completely external computer at a customer's or partner's office."

"A virtual working environment lays the foundation for enhanced IT security by protecting business-critical or integrity-protected data. PKI and smart cards offer a cost-effective and user-friendly complement for identifying and authenticating the system's end users in a consistent and uniform manner."

Virtualization boosts IT security

We began by noting how one of today's greatest IT challenges is related to the need for qualified IT security in an increasingly mobile and flexible world. A virtual desktop can help reduce costs and increase user flexibility. It can also help lay the foundation for increased IT security, without compromising on accessibility and user-friendliness.

Traditionally, corporate information and business support applications were distributed to all employee terminals and stored locally. Distributed and locally stored data increases vulnerability and the risk of hacking, which leads to relaxed security. With virtual desktops, all information and applications are instead stored centrally. This improves the chances of protecting data, making backups and restoring lost or damaged information.

Applications and services in the virtual IT environment are made available for the organization's end users based on predefined user profiles and central policy decisions. When a work session ends and the virtual desktop shuts down, the session and all its information goes back to the central, protected data center. A desktop that is shut down cannot be infected by malicious code. In a virtual work environment, where all applications and data are stored centrally, a lost or stolen laptop no longer poses a major security risk.

A virtual work environment can thus become an important cornerstone for protecting business-critical or integrity-protected data in all types of organizations: healthcare, the financial sector, private businesses and public agencies. However, for a complete security solution, protecting information and data in a qualified manner is not enough. Ensuring that the right individuals have access to the data is just as important. The solution must therefore also be able to identify and authenticate the end user in a consistent and uniform manner, regardless of where they are located or what terminal they are using.

In this regard, the combination of Public Key Infrastructure (PKI) and smart cards is a safe, cost-effective and user-friendly alternative.

PKI and smart cards – the road to better security

As security challenges increase for companies and organizations, qualified solutions based on the combination of PKI and smart cards have made huge inroads.

By combining technology, processes and standards, PKI offers:

- **Authentication** – strong asymmetrical two-factor authentication
- **Non-repudiation** – proof of the integrity and origin of data through digital signing
- **Integrity protection** – prevents unauthorized interception of communication
- **Confidentiality** – only authorized recipients can access the information

Two encryption keys are directly linked to the sender of the information (a person, an IT service or an application) and the recipient. The information is guaranteed to be free from interception, so-called man-in-the-middle intrusions, and cannot be read by anyone other than the intended recipient. This allows information to be exchanged over a fundamentally insecure network such as the Internet, without the risk of unauthorized views.

Another cornerstone of PKI is that authorized users need to be able to clearly identify themselves for the system and the services available, while providing information on their unique encryption keys. This is handled by individual, personal certificates, which contain information about the user and its public key. The certificate is preferably stored on a smart card and is mathematically linked to the private key on the card. The private key can only be used by someone who knows the card's PIN code. Smart cards are small and completely mobile and, unlike a computer hard drive, they can easily be brought along when the user is leaving the workplace. Combining different features on the card, such as key-card entrance, personal ID and follow-me printing increases the incentive for employees to actually take the card with them when they leave their computer.

The user logs in to the IT environment with a combination of a smart card and a PIN code. This gives "two-factor authentication," a combination of two things: information from the user with something that they physically hold. By combining two-way SSL, two-factor authentication, and the use of smart cards with hard certificates, PKI and smart cards offer one of the strongest alternatives for a secure IT environment on the market.

"By combining two-way SSL, two-factor authentication, and the use of smart cards with hard certificates, PKI and smart cards offer one of the strongest alternatives for a secure IT environment on the market."

Net iD Enterprise from SecMaker

Net iD Enterprise from SecMaker is the market's most qualified software for handling smart cards and certificates. Net iD Enterprise offers full support for authentication, encryption, and digital signing, and is one of the IT sector's strongest and most user-friendly security solutions.

Net iD Enterprise is based on open international standards and documented interfaces. This ensures that the solutions perform optimally

"In addition to enhanced security, Net iD Enterprise also offers a range of features that improve flexibility and ease of use for the organization's end users: single sign-on, automated processes and session roaming."

regardless of platform or operating system: Windows, Linux, Novell NetWare, Mac OS X, Microsoft Terminal Server or Citrix. Standardized application interfaces enable the integration of Net iD Enterprise with applications and services, such as MS Active Directory, VPN solutions, web applications, and business support systems: EMR systems, POS systems, etc.

All in all, this means that Net iD Enterprise can be integrated with virtually any target environment without costly and time-consuming customizations.

Net iD with Citrix® XenDesktop™ and Citrix® XenClient

The modular architecture of Net iD Enterprise also enables customization to a virtual environment. Just as operating systems and applications can be virtualized and managed centrally while at the same time made available to each individual employee, the Net iD client software can also be virtualized. The client software is decoupled from the physical workplace and the smart card reader, and is run as a virtual client in a central server in the company's data center.

This means that Net iD Enterprise can be used to great advantage to strengthen security in virtual environments. The client doesn't need to be installed on the local PC, thin client or handheld device. Instead, the card reader is emulated through virtual channels via PC/SC to the server and all applications and features that are normally offered on the local client are available in the virtual environment.

In addition to the improved security through PKI in combination with smart cards, Net iD Enterprise integrated in the virtual Citrix environment offers a range of features that improve usability for the organization's end users:

- **Single Sign-On** – Net iD Enterprise offers full support for Single Sign-On (SSO) to the virtual environment. By inserting their smart card in the card reader and entering a personal PIN code, users receive direct access to Citrix-published applications, web-based systems and other target systems that require login with certificates. This gives the user quick and easy access to their complete virtual work environment of software and features without needing to remember or enter several different passwords.

- **Automated processes** – In mobile environments, such as in healthcare, it is common for several users to share a single computer and have the need to quickly and effectively access confidential data from different workstations. Here, PKI and smart cards offer a simple and efficient complement to the virtualized environment through automated processes. For example, automatically shutting down all the underlying virtualized applications when the user takes out their smart card from the terminal protects services and information against unauthorized access without requiring the user to manually log out of different applications.

- **Session roaming** – Similarly, Net iD Enterprise integrated with the virtual environment offers support for session roaming. When the user pulls the card out of the reader for a break or to move to different workstation, the session automatically returns directly back to the server. Back at any workstation, the user can resume work in the same session by inserting their smart card and entering the PIN code. The applications and the documents will be there waiting, just as they were at logout.

In summary, Net iD Enterprise and smart cards represent a powerful addition to the virtualized Citrix environment by both offering greatly improved IT security and by introducing new opportunities for user-friendly services in a modern, mobile work environment.

Summary

As employees become more mobile and corporate geographic boundaries become more relaxed, IT managers face greater and more complex challenges than ever before. An increased rate of change in organizations and companies, combined with new requirements to support an increasing number of combinations of applications, services, operating systems and terminals has prompted many IT managers to re-evaluate their IT environments from the ground up. This often results in a transition to a virtualized work environment.

In a virtualized environment, operating systems, applications, and data are abstracted from the individual employee's workstation and terminal and centralized into a single data center. A virtualized IT environment enables optimization of the organization's IT investments as well as the operational costs of IT administration and support. The central management of platforms and applications often contributes to a much faster introduction of new services and updates to the organization's end users.

Yet another IT challenge associated with an increasingly flexible work environment is the growing need for qualified IT security. In a virtualized environment, all information and applications are stored centrally. This improves the chances of protecting data, making backups and restoring lost or damaged information, and lays the foundation for enhanced IT security. However, a complete solution also requires a consistent and uniform method for identifying and authenticating the end user in the solution.

PKI and smart cards offer a safe, cost-effective, and user-friendly alternative for qualified security by providing support for authentication, non-repudiation, integrity protection, and confidentiality. By combining two-way SSL, two-factor authentication, and the use of smart cards with hard certificates, PKI offers one of the strongest alternatives for a secure IT environment on the market.

Net iD Enterprise from SecMaker combines PKI with smart cards. The modular architecture of Net iD Enterprise enables full integration of the system into a virtual environment. Through a series of additional features, Net iD Enterprise also helps to improve usability and simplify the everyday work of the organization's employees to ensure that enhanced security and usability go hand in hand.

1306#212-01ENG

Hesselmans Torg 5, 131 54 Nacka, Sweden
+46 8 601 23 00
info@secmaker.com www.secmaker.com

secmaker