DUTCH CENTRAL JUSTICIARY COLLECTION AGENCY

Government agency boosts efficiency and drives down costs with RSA technology

AT-A-GLANCE

Key Requirements

- Enable employees to work remotely with reliable access to the company desktop environment
- Replace the inefficient PKI-based remote authentication model with more reliable, user-friendly two-factor authentication
- Ensure the new model is easy to install and run, and compliant with the ISO 27002 standard

Solution

- Two-factor authentication with SMS tokens are provided by RSA SecurID® and Authentication Manager 8
- The solution integrates seamlessly with VMware virtual desktop environment
- Implementation was completed in half the anticipated time, with support from PointGroup

Results

- ROI was achieved within just three months, with an annual saving of nearly €100,000
- New users can now be set up in minutes, rather than weeks
- Self-service makes management of the solution more efficient for users and service desk
- Virtual desktops enable employees to work more flexibly on a device of their own choice

"We've found RSA SecurID® and RSA Authentication Manager 8 to be a highly cost effective and trustworthy authentication solution for our virtual desktop environment. Employees can now access their work from anywhere, while the service desk has seen its administrative burden reduced."

CHRIS EYZENGA, SECURITY AND CONTINUITY MANAGER, CJIB

Part of the Dutch Ministry of Public Safety and Justice, the Central Justiciary Collection Agency (CJIB) manages the recovery of all penalties and fines on behalf of the Ministry. It employs around 1,100 people, who are committed to their role in upholding the integrity of the Dutch justice system.

KEY REQUIREMENTS

The remote access solution that the agency had in place was based on a Public Key Infrastructure (PKI), which over time had become problematic for the IT security manager. Chris Eyzenga, Security and Continuity Manager at CJIB, explains: "The PKI-based model offered us limited support for devices that weren't based on the Windows operating system. It required additional shoring up of our remote security systems, which limited the functionality available to employees. It also took up to eight weeks for keys to be issued to new users, or if an existing user needed a replacement. Needless to say, this was very inefficient for the organization, and inconvenient for our employees, who need constant, reliable access to email, documents and spreadsheets."

The agency therefore began to look for a new remote access solution with two-factor authentication that would align with the ISO 27002 security standard and also be easy to install and use.

SOLUTION

CJIB began by running a proof-of-concept of a desktop virtualization solution from VMware. "The solution worked well, but we needed to add two-factor authentication to ensure we had the level of security we needed," says Eyzenga. "We knew that RSA SecurID® and Authentication Manager 8 integrated seamlessly with the VMware solution, so we wanted to use them to deliver the additional authentication."

Next, the agency needed to decide whether to use hard or soft tokens. It contracted local RSA partner, PointGroup, which ran a cost comparison which showed the soft token option would be more economical for CJIB. The agency decided to use SMS tokens delivered to employees' personal mobile phones. "No one goes anywhere without their phone these days," says Eyzenga. "So by sending their authentication tokens to these devices, we can be sure the employee will always be able to access it, and it minimizes the risk of them forgetting or losing their token." PointGroup and CJIB worked with local network provider CM Telecom to negotiate a secure, reliable network over which to send the SMS tokens.

With the arrangements in place, the agency ran a pilot of the new remote desktop solution, which demonstrated its simplicity, ease of use and scalability to the rest of the organization. Eyzenga recalls: "The installation was very quick. We'd planned two days for it, but we were done by afternoon tea on the first day. It was also easy to set the parameters we need in order to align with the ISO 27002 security standard, such as those around the lifetime of SMS tokens and imposing limits for the number of times an incorrect PIN number can be entered before an account is blocked."

"We achieved return on our investment in the RSA solution in just three months and have seen an annual management saving close to €100,000 following an investment of just €42,000."

CHRIS EYZENGA, SECURITY AND CONTINUITY MANAGER, CJIB

RESULTS

The agency achieved full return on its investment in the RSA solution within three months. "We've seen an annual management saving of €100,000 following an investment of just €42,000," says Eyzenga.

The time savings have been significant for everyone included. Whereas it would take up to eight weeks to set up a new user previously, it can now be done in a matter of minutes. "We simply need to check a box in our Active Directory, then the user can self-serve to set up the SMS token client on their phone and they're ready to go," Eyzenga explains. "Moreover, it's easy to set up on the majority of platforms, including Windows, OSX, iOS, Android and Linux environments."

The increased support for self-service also means that the service desk can work much more efficiently as it does not have to deal with lost or broken tokens, or with supporting users in restoring their broken PKI-based remote authentication, which was affected by updates to the environment (JAVA and underlying operating system).

Feedback from the 300 road warrior and senior management employees that are using the new solution has been very positive. "Having access to their virtual desktops from any location means that they can achieve a more favorable work-life balance," Eyzenga says. "They can start working on something in the office then leave to pick up their children from school, for example. Then they can log on again from home that evening, and the cursor is still blinking exactly where they left it."

LESSONS LEARNED

Eyzenga has already started speaking with other agencies in the Dutch Ministry of Public Safety and Justice, many of which are interested in replicating the remote working model. He shares advice based on his own experience, including:

– If using SMS tokens, it's important to ensure the path over which they will be delivered is secure and reliable. "We felt that 3G was not secure enough, and 4G is not yet ubiquitous, so the support of PointGroup was essential in developing a solution here," says Eyzenga. "You also need to ensure that you have additional measures in place to fill any security gaps in the network. For example, we set rules for the RSA SecurID and Authentication Manager 8 token codes so that they expire after two minutes or after use."

– Local expertise is also highly valuable, and CJIB benefitted from working with an approved RSA partner. “PointGroup could offer insights based on its own experience and deep knowledge of the RSA solutions we were implementing,” Eyzenga says. “This meant we could be up and running in minimal time.”

– PIN codes are just as important as token codes. “They’re one half of the two-factor authentication process, so it’s important to make sure they’re as robust as the tokens,” Eyzenga explains. “We’ve set restrictions here too, so for example regular numeric patterns like 1234 are not allowed. We also prevent employees from re-using a certain PIN too frequently.”

– Putting power in the hands of the users can drive significant efficiency improvements. “We found the self-service element of Authentication Manager 8 to be very beneficial,” says Eyzenga. “Employees can change their own PIN codes and carry out general admin on their own accounts without having to raise a service desk ticket. This means they get what they need much faster, and it takes pressure off the service desk.”

CONTACT US

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.emc.com/rsa.

www.emc.com/rsa

EMC²

RSA