OneSpan

CASE STUDY

CITY OF COPENHAGEN

CITY SECURES LOGON WITH ONESPAN MOBILE AUTHENTICATOR SMS

EXECUTIVE SUMMARY

Business Objective

Protect citizens' confidential information when using Outlook Web Access to remotely access the city's network and applications.

The Problem

Replace static passwords with one-time passwords (OTPs) that could be sent as text messages (SMS) to employees' mobile phones

The Solution

- Digipass® 250
- Digipass 275
- Digipass GO 6
- OneSpan Authentication Server

Results

- Favorably received by users
- Low total cost of ownership
- Mobile usability broadened employee acceptance

The city government of Copenhagen cares a lot about the security of its citizens' confidential information. For years, they have been investing in strong authentication to protect the login procedure to the internal network and Outlook Webmail. Static passwords are banned and replaced by one-time passwords sent as text message (SMS) to the employees' mobile phones.

Employees working for the City of Copenhagen deal with confidential information about citizens and the city's funds. The information is stored on an internal network. Of course, it is of the utmost importance that this network is securely protected. Nowadays, 6,600 users log on with SMS using OneSpan Mobile Authenticator SMS, a very user convenient solution for the users.

A Bit of History

The city of Copenhagen and OneSpan have already shared a long history together. Their cooperation started in 2003, when the city started to use OneSpan's server for secure remote access. The server was a part in a shared environment, hosted by an external company. Later on, the security regulations promulgated by the City of Copenhagen mandated that Outlook Web Access (OWA) had to be secured with strong authentication. The authentication requests for both secure remote access and Outlook Web Access were verified by one and the same server. In 2007, a new and separate OneSpan project was started up to add two-factor authentication to a large Citrix environment. A second server was installed, hosted by City of Copenhagen itself.

In 2009, the City of Copenhagen merged these two environments into one. OneSpan Authentication Server hosted by the external company and the OneSpan Authentication Server hosted by City of Copenhagen were merged into one single environment with one central administration.

Always Near

In a first phase, City of Copenhagen implemented OneSpan's Digipass GO 3 to add strong authentication. This one-button device generates a one-time password by a simple press on the button. However, strong authentication with SMS is sought-after in Denmark these days. City of Copenhagen appreciated this solution's user-friendliness and ease of use. The fact is that employees tend to forget another extra device, whereas they always carry their mobile phone with them. That is why City of Copenhagen changed to OneSpan Mobile Authenticator SMS.

Andreas Hare, Head of Division IT-infrastructure at City of Copenhagen, explains why they opted for OneSpan Mobile Authenticator SMS: "On the one hand, we noticed that our employees often forgot or lost their Digipass device. Conversely, they always take their mobile phone with them. On the other hand, the scalability of this solution was a major asset. In the last couple of years, the number of users has grown and this was easily adapted with OneSpan Mobile Authenticator SMS.

How it Works

Instead of logging on to their Outlook Web mailbox or to the internal network with an unsafe static password, the employees of City of Copenhagen use a method called two-factor authentication. This means that two elements have to be involved: something you have – in this case a OneSpan Mobile Authenticator SMS to obtain a one-time password (OTP) – and something you know, such as a personal static password.

When the City of Copenhagen's employees open their login screen, they insert their username and personal static password. After entering these credentials, OneSpan Authentication Server is triggered to send an SMS with an OTP to the end user's mobile phone. Only when the OTP is inserted, access to the applications is granted.

Every user's mobile phone with Virtual Digipass is imported into OneSpan Authentication Server's database and is assigned to the user. In the back-end, OneSpan Authenticaiton Server checks whether the person who sends the request is the right one to log on. The OTP is only valid for a limited period of time. After 32 seconds it becomes invalid, which makes it impossible to intercept and reuse the password.

Local Experience

It was a multi-level implementation that started in 2003 and went through different stages. A number of difficulties such as naming standards or merging user databases were overcome with a very limited user impact. All development was done by Danicon ApS, a Danish OneSpan partner. Danicon has worked closely together with the OneSpan Support Department in Belgium.

Danicon has a large asset: it has an in-house OneSpan Certified Engineer. Steffen Petersen was schooled by OneSpan SEAL (Security Experts Academy & e-Learning platform) and is permitted to implement OneSpan's solutions and provide adequate and thorough support to the City of Copenhagen. Next to this local embedding, it is also interesting for Danicon – and by extension for City of Copenhagen – that Mr. Petersen is a member of the OneSpan SEAL community. In this peer group, information about the latest IT security technologies, evolutions and threats are typically exchanged. As a result, a OneSpan Certified Engineer stays up-to-date on the security trends and maintains his knowledge at the highest level.

Andreas Hare, Head of Division IT-infrastructure at City of Copenhagen, is happy with the integration of OneSpan Mobile Authenticator SMS. "Things are running very well," he says. "Our employees always have their authentication device with them and we are contented with the benefits this OneSpan technology offers: an excellent balance between price and quality, scalability and of course, the solution's ease of use."

Partner Overview

Danicon is a Danish IT consulting company with extensive experience in provisioning of high-quality IT solutions across a variety of platforms and business areas. Danicon's primary customer base consists of companies with 100 to 500 employees, but it has also both smaller and larger companies. Danicon also has an in-house Certified OneSpan Engineer, which enables them to offer customers OneSpan's secure authentication and digital signature solutions.