

SSH Communications Security provides Secure Remote Access for Administrators of a Major Asian Government Agency

A government agency in Singapore needed a flexible and easily-deployed secure authentication solution for its system administrators. SSH solutions allowed the organization to ensure that the right people had access to its mission-critical data with minimal intervention.

Wanted: Low-Impact Two-Factor Authentication

As a state-owned organization managing confidential stakeholder information, the customer wanted to boost the level of security required for its administrators to access the company infrastructure. Administrators were already using a VPN (Virtual Private Network) setup, but the state body wanted to enforce an additional layer of security.

The answer lay in implementing a two-factor authentication solution that would result in little or no disruption to ongoing operations or the work of the system administrators. Furthermore, the chosen solution also had to integrate smoothly with the VPN system already in place.

As such, a token-based two-factor solution was not a viable alternative, as it would incur high costs and a large investment in effort for deploying and managing physical tokens, registering and de-registering them, and finally in decommissioning and recycling expired tokens at the end of their life spans.

In addition to these factors, decision-makers also considered the end-user experience, and concluded that it would deteriorate if users had to carry and account for physical tokens. The potential for lost tokens and the resulting inconvenience in replacing them was also considered.



Unparalleled Usability, Scalability and Flexibility

After reviewing the alternatives, officials at the agency decided to evaluate SMS and email solutions. SSH MobileID emerged as a clear frontrunner in the appraisals based on its cost-effectiveness, ease of deployment and use, and scalability. SSH Mobile ID provides customers with significant cost savings in the form of virtually no administrative expenses, not having to provision physical tokens, and no additional costs involved in scaling up the number of users.

The decision to deploy SSH was based on:

Easy Deployment

SSH MobileID could be integrated with the existing VPN solution quickly and seamlessly, without any disruption to existing infrastructure.

Enhanced User Experience

Users do not have to carry an additional piece of hardware and can rely on existing mobile devices for secure authentication. The company also found that users could be instantly activated and suffered no delays in accessing critical infrastructure. The result was a high acceptance level to the new authentication demand.

Unmatched Manageability and Scalability

SSH MobileID is effortlessly implemented and managed – no other solution offers such simplicity on adding and/or removing users, making it easy to rapidly scale up to much larger numbers of users on demand.

Cost and Operational Efficiency

With no tokens to provision, manage or replace SSH MobileID was by far a more cost-effective alternative than traditional hardware-based solutions. Moreover no additional costs are involved in adding new users and license and user fees are not incurred for inactive accounts.

Moreover, this creative solution allows organizations to activate user accounts on an ad-hoc basis or even pay-per-use, ensuring that they don't have to pay license and maintenance fees for inactive users.

SSH MobileID also proved to be the optimal choice from the end-user perspective. The institution wanted to ensure smooth and easy adoption of the supplementary authentication routine. With no additional physical device involved, instant activation, an intuitive approach and decreased waiting time to access organizational resources, SSH MobileID enhanced the user experience.

Using the SSH solution, the organization was able to ensure that there was no resistance to its program to introduce two-factor authentication for access to its critical infrastructure. The fact that system administrators did not need hardware tokens but could use their existing mobile devices ensured a high user acceptance level when the solution was rolled out.

The customer was also pleased with the simplicity with which the solution was implemented and managed, in particular, the ease of adding/removing and registering/de-registering users. Additionally, because of the solution's flexibility and scalability, plans to scale up to a larger number of users could be easily implemented.