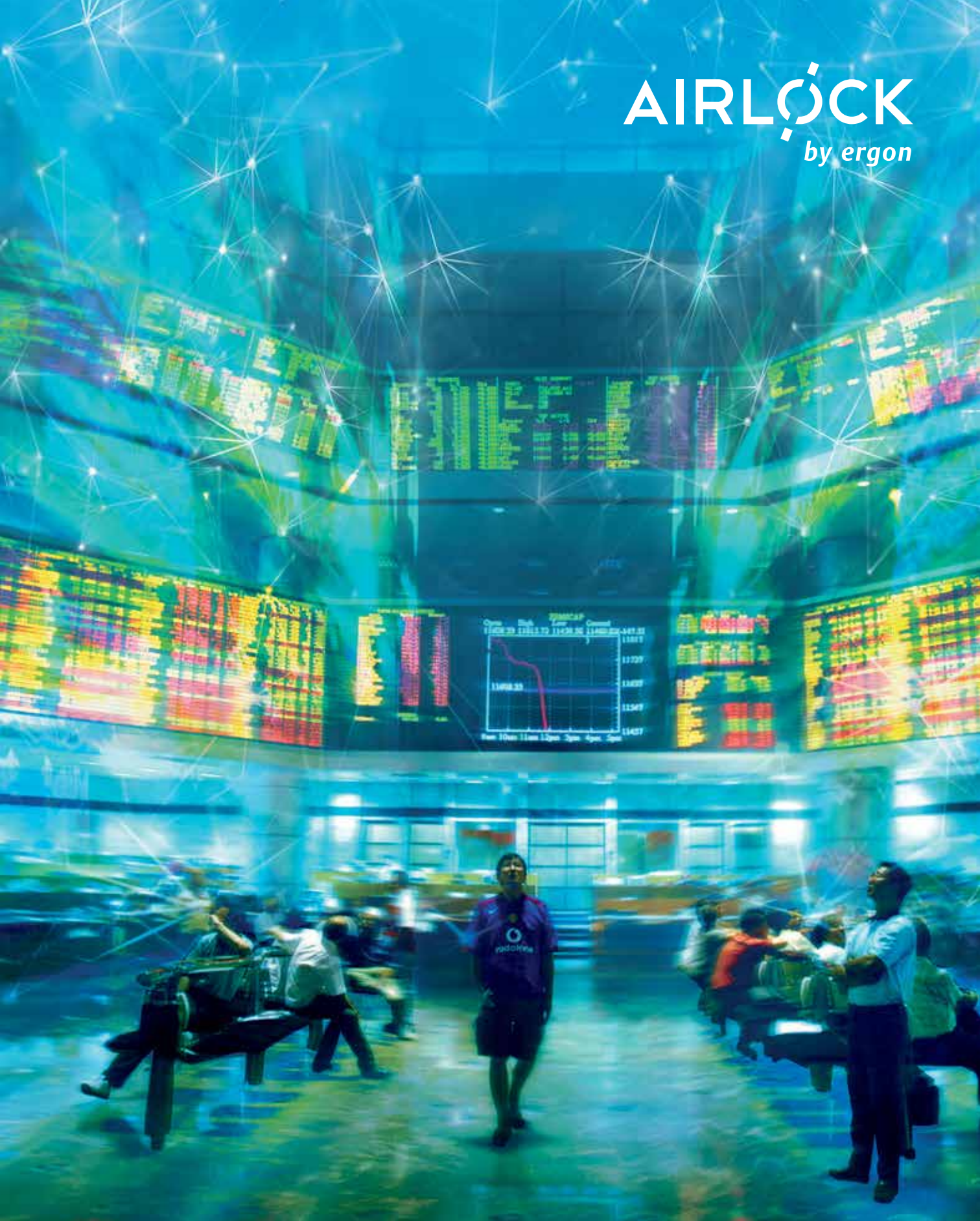AIRLOCK
by ergon

Swiss Post

E-health platform vivates

Swiss Post, the Swiss postal service, doesn't just deliver letters and packages. It is increasingly reinventing itself as a one-stop service provider, transporting information reliably and sustainably and adding value. From this starting-point, Swiss Post set itself the goal some years ago of developing an e-health system that would allow the various parties involved in the healthcare sector to exchange patient data securely—and to ensure that the integrity of such sensitive information is guaranteed at all times, Swiss Post is turning to Ergon's Airlock Suite for its vivates e-health system.

Secure patient data

Patients often move between different service providers—they might have a general practitioner who refers them to a specialist, for example, who will then determine that a surgical procedure is required, resulting in an in-patient hospital stay. At the moment, patients often have to cart their information (X-ray images, for example) from one doctor to the next themselves and are routinely subjected to the same questions again and again. A case notes dossier that can be accessed by every attending physician and where examination results can be recorded will ease this process considerably.

Patient data is a sensitive business, however; nobody wants the world to be able to look up their medical history. Health data is protected in Europe as a "special category of processing", which means that the security requirements are even stricter than for banks; access must be granted on an individual basis to each party involved. This authorization is carried out either by the patient or via the assignment system: anyone uploading documents to the dossier will simultaneously determine who may view the information, and thus implicitly authorize the recipient. The patient retains control of access rights at all times and can decide who may view the documents.

Access in an emergency

Guaranteeing safety in the healthcare system is not just a matter of ensuring confidentiality, however. In the event of an emergency, it is essential that a doctor has immediate access to all relevant patient data, to prevent potentially fatal consequences for the patient. Unwittingly giving someone a medicine to which they are allergic, for instance, can trigger a dangerous reaction. But vivates has a solution for this too; the doctor can declare an emergency and will then be allowed unlimited access to the data for a restricted period. To prevent misuse, both the patient and an independent examining doctor will be alerted whenever such a call is made.

A flexible authentication layer

The vivates e-health platform was tested in four districts in the Canton of Geneva and then rolled out in additional cantons in 2013. It soon became apparent that the authentication solution used provided the requisite levels of security but its flexibility and manageability left something to be desired in respect of the challenges it was likely to face in the future. Switzerland's federal system means cantons have slightly different laws, and accommodating these disparate authorities was proving to be too expensive and time-consuming. As Michael Doujak, Head of vivates Development for Swiss Post, explains: "Our system must be easily scalable, as every customer's circumstances are different and thus each of them presents new or distinctive challenges. So we can't install the authentication layer the same way for every client, we have to be able to provide customized configurations, and that's where an automated management system is a great help."

Hospitals and healthcare organizations usually have their own ID token system (SuisseID, IDP or a proprietary system, for example) and each organization should be able to retain its token for the case notes dossier. "The term we use here is 'transferable trust'; the healthcare sector knows its staff and manages access, so no duplication of the ID procedure is required," continues Michael Doujak.

Furthermore, a broad spectrum of parties is involved, from a large hospital with its own IT department, through smaller organizations like pharmacies, to single individuals (an independent doctor, or even the patients themselves); all of these will require access to the system. There were also tough design challenges to be faced—the landing page had to be attractive and user-friendly but also adaptable to different sets of circumstances.
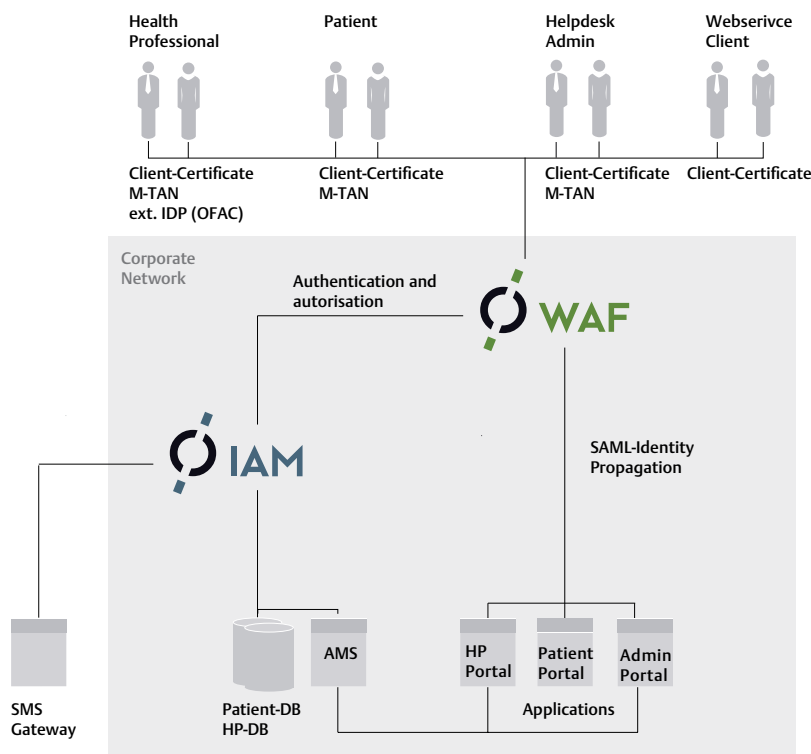

«There are more authentication solutions than we initially anticipated," says Michael Doujak, "but we were nonetheless able to bring this phase in on time and on budget as well—which is seldom the case with such large IT projects.»

Michael Doujak, Head of vivates Development for Swiss Post

Plug-in functionality is the decider

After Swiss Post had inspected a range of Swiss service providers and tested their technology, they made their choice for Ergon's Airlock Suite. What swung it in part was the high plug-in functionality with all kinds of different identification systems that Ergon had already demonstrated in previous

Figure 1 Michael Doujak, Head of vivates Development for Swiss Post

Figure 2 vivates infrastructure

projects, ensuring compatibility. Other points in Airlock Suite's favor were its uncomplicated administration, its flexible operation in different configurations and its ability to hot-swap upgrades (especially for security patches). With Airlock WAF serving as an authentication layer for patients, doctors, service providers and administrators, and Airlock IAM managing identities, this separation of authentication and identity propagation permits great flexibility when accessing the system.

Ergon's e-health project broke new ground, and the specific requirements of the healthcare sector brought their own special challenges: a number of external, non-standard IDPs, such as OFAC, had to be integrated. "We were encountering a lot of use cases for the first time here," concedes Adrian Berger, one of Ergon's Heads of Department. "These included the representation of people who were not compos mentis (so-called "dual carding", where two SSL sessions have to be able to run simultaneously) and of course emergencies, where certain data has to be available immediately."

On time, on budget

Despite the complexity of the subject matter, the development scheduling was tight: the project was tendered in March 2013, evaluation started in May and the old security platform was due to be scrapped by year-end. Keeping to this timetable meant dividing the project into two phases: the scope of the first, which was completed on time and on budget in December 2013, was scaled back in respect of the authentication tokens used, with only a smart card being created. The second phase saw the integration of numerous other authentication solutions. "There are more than we initially anticipated," says Michael Doujak, "but we were able to deliver this phase on time and on budget as well—which is seldom the case with such large IT projects." Development is yet to be completed, however. "The further we roll out the dossier, the more challenges we encounter," he continues.

Focusing on flexibility
Interview with Adrian Berger, Ergon's VP Finance

What's special about the security of an e-health platform?
The prerequisites are stricter, even compared with banks and insurance companies; data protection is more rigid and more closely regulated. This said, there have to be mechanisms in place for emergency situations, such as when a doctor needs immediate access to data to save a life, for example, and this duality has made the project very exciting—it has been a learning experience for us.

What changes can users expect from the migration?
None, for the moment—and that was precisely the point of the project. The existing solution has been replaced in such a way that all previous means of authentication can still be used; the changeover would probably not have been accepted by the end-users in any other circumstances. We have nonetheless been able to lay the groundwork for even greater flexibility in the future, including authentication solutions via mobile phone, for example. These have already been integrated and have gone live.

How important has the flexibility of the solution been to this project?
You might say flexibility has been the core issue. The Swiss healthcare sector is highly segmented, and our solution reflects this. For one thing, each canton has slightly different legal infrastructure that has to be accommodated, so we are working with a range of separate authorities, and there are also plenty of organizations with their own security tokens. The Aarau Cantonal Hospital has its own PKI solution, for example, which we are integrating. One important criterion was that the solution should be easily scalable in breadth, and Airlock Suite's flexibility makes this possible.

Ergon Informatik AG
Merkurstrasse 43
CH–8032 Zürich

+41 44 268 89 00
www.airlock.com
twitter.com/ErgonAirlock

smart people – smart software

Founded in 1984, Ergon Informatik AG now has workforce of 235 and numbers among the most long-standing and successful IT service providers in Switzerland. Over 80 % of our employees are graduate software developers, and most of them have trained as IT engineers at the Swiss Federal Institute of Technology (ETH), Zurich—one of the world's top ten universities. Ergon Informatik AG has also won multiple awards for its sustainable personnel policy.

Ergon Informatik AG is a broadly diversified company that provides services to a wide variety of sectors. Ergon has exceptional expertise in sectors such as financial services, eBanking, telecommunications and security. In 1997, Ergon developed Switzerland's first eBanking system. Airlock Suite, our security product, was launched on the market in 2002 and is now used by 300 customers around the globe.

For more information visit www.ergon.ch