

## Questions and answers regarding the merger of Swisskey Ltd. with Payserv Ltd.

The issuing of Swisskey ID products and the Swisskey SafeCard to the general public was discontinued on 7 May 2001. The company Swisskey Ltd. was absorbed by Payserv Ltd. on 30 June 2001 and discontinued all services as of 31 December 2001.

**All certificates were definitively blocked after 31 December 2001!**

### **What are the direct consequences of the merger of Swisskey Ltd. with Payserv Ltd.?**

The issuing of digital certificates to the general public has been discontinued. This affects all Swisskey ID products (Personal ID, Corporate ID, Server ID, WAP Server ID and Code ID).

### **Which services will continue to be available after 31 December 2001?**

Only the definite Certification Revocation Lists (CRL's) can be downloaded under [www.swisskey.com](http://www.swisskey.com)

### **Where can I obtain a certificate when Swisskey no longer provides this service?**

There is no longer a public certification authority in Switzerland for digital identities. Companies that also issue certificates are:

Telesec (German Telecom)	<a href="http://www.telesec.de">www.telesec.de</a>
TC Trustcenter (Germany)	<a href="http://www.tctrustcenter.de">www.tctrustcenter.de</a>
Verisign (USA):	<a href="http://www.verisign.com">www.verisign.com</a>
Thawte (South Africa):	<a href="http://www.thawte.com">www.thawte.com</a>
WEB.DE Trustcenter (Germany)	<a href="http://trustcenter.web.de">trustcenter.web.de</a>

A list of all certification authorities is available at: [www.pki-page.org](http://www.pki-page.org).

A list of the accredited certification service providers in Germany is available at: [www.regtp.de](http://www.regtp.de)

### **I use a Swisskey certificate to authenticate myself on the Web. How will I continue to receive access to these applications?**

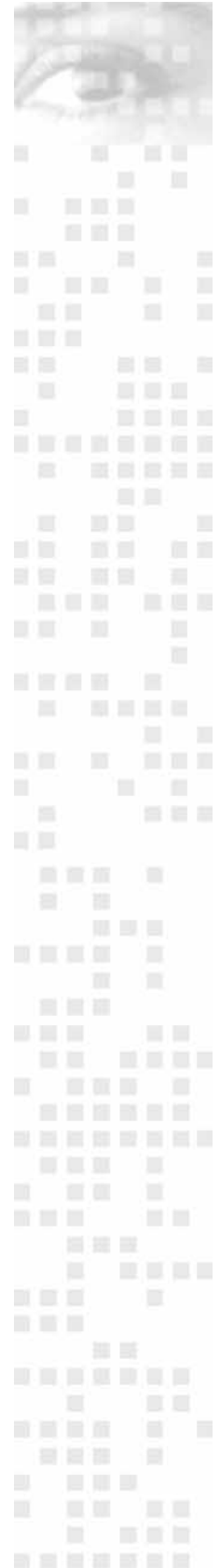
Contact the service provider. They will be able to offer you alternative authentication methods so that you can continue to receive unlimited access.

### **What will happen with e-mails that have been encrypted with a Swisskey certificate and then saved. Will I be able to continue to read or decrypt these once the certificate has been blocked?**

Yes, as long as the certificate is installed in the browser or e-mail program, all messages that have been encrypted with it can still be read, even when the certificate is definitively blocked. However, we recommend that you also store important e-mail unencrypted in a secure location in any case.

### **Although the certificate is blocked, it continues to exist in my browser or e-mail program. Thus, I could continue to send digitally signed messages and my communications partners can continue to send me encrypted messages.**

This is theoretically possible. However, it makes no sense to continue using these certificates. Since Swisskey has discontinued the public service, the certificates can no longer be verified.



### **How do I proceed if I wish to continue to use certificates in our organization?**

Either you seek out another provider, or you construct your own company in-house CA.

### **Why was Swiskey discontinuing the issuing of digital certificates now in particular?**

The demand for digital certificates in Switzerland has yet to reach expected levels, and for a variety of reasons also will not do so in the near future. In the international environment as well, the indications are that the demand for branch-independent, universally applicable certificates will not reach a level quickly enough to cover the costs of issuing and administering IDs for the digital world. There is a wide ranging lack of attractive offers and solutions on the Internet that are based on digital certificates. This situation can be primarily traced back to the high degree of complexity involved in such a project. There is no alternative to PKI technology, however its dissemination will take longer than originally foreseen.

### **What remains of Swiskey's basic idea of issuing universally applicable certificates?**

For the time being there will no longer be any universally applicable certificates for the general public. Solution providers will issue their own certificates to their customers, which then can be used in specific applications.