EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Summary of audit findings

The SFAO has audited the Admin PKI – the basic infrastructure and offering for the issuing of digital certificates – within the Federal Office of Information Technology, Systems and Telecommunication (FOITT). The examination concentrated on assessing the development and current operation as well as future prospects. Admin PKI refers to all processes and the hardware and software needed for issuing certificates of different grades.

After a tumultuous and somewhat unfortunate start to the Admin PKI (cf. Chapter 4), the FOITT managed to build up the infrastructure and processes needed to offer the Federal Administration, the Cantons and Municipalities the certificates they require for their applications. Apart from the Class A to D certificates defined within the Federal Administration, the FOITT can also offer specific customised certificates to meet the needs of customers or their applications. Through KPMG certification for Class A (ZertES-compliant) certification services, which is expected in the second quarter of 2007, the Admin PKI and thus also the FOITT will have proven their capabilities and quality at the highest level. With the issuing of some 25,000 certificates to the Cantons in 2006 the Admin PKI proved its maturity. At the time of the audit, over 40,000 certificates in various forms were in use.

The FOITT is now recognised by all Cantons and by the Swiss Information Technology Conference (SITC) as the leading provider of digital certificates. In addition to the SSO Portal, other large-scale applications using these now or in the near future include the information system for placement and labour market statistics (AVAM), electronic customs declarations (e-dec), and the sending of encrypted signed e-mails (Secure Messaging). The certificate prices are not of central interest, given that they are competitive and reasonable. Due to the slow start in developing the present Admin PKI, it is difficult to draw up a fair profitability analysis for the investments made so far, amounting to some CHF 12 million. The main benefit of a PKI lies with the customer, i.e. the applications, as a high level of security can be obtained using simple means. The potential for issuing more certificates is thus correspondingly large. The sale of certificates should cover the operating costs and technical updates. Although certain alternative security options would be less costly, this would hamper the heterogeneity of large eGovernment solutions. The PKI technology available from the FOITT provides for standardised solutions across all administrative levels, and even across all of Switzerland through cooperation with other ZertES-compliant providers, such as Swiss Post with its IncaMail product. While the Cantons are free to procure certificates from other providers, they are very likely to reuse the Admin PKI certificates already in use. The other ZertES-compliant providers on the Swiss market (Quo Vadis, Swisscom and Swiss Post) are potential partners for the FOITT as cross certification could be implemented in many eGovernment solutions.

Numerous studies have been carried out on the need for PKI solutions in Switzerland. A nationwide overview of the Classes A to D defined in the Federal Administration is not possible, however, as other providers have defined their own certificate classes. Given the widespread use of certificates in the public sector, this will then become a matter of course over time, creating further momentum beyond the Federal Administration. The costs will remain constant but will be distributed over substantially more certificates than today. Class A certificates are the only ones in Switzerland governed by law. However, their potential use is regarded as limited, as only very few legal transactions (e.g. advance payment contract) call for a handwritten signature, which would be equivalent to a qualified electronic signature. However, this certificate – having been tested for quality by its certification – forms the basis for the general trustworthiness of the provider himself. The SFAO thus believes it makes absolute sense for the FOITT to be able to offer this class.

Today, the FOITT enjoys very high expectations of and trust in its certificates. In the future, as now, the requirements for certificates will be determined not by a shared, centralised knowledge base but by customers' wishes. The FOITT has proven that it can meet the organisational and technical requirements of a Certification Service Provider (CSP). ZertES certification concerns not just the Admin PKI but the entire FOITT, impacting upon its processes, documents, infrastructure, etc. With its strong service offering, high availability and proven quality, the FOITT is in a position to build upon the trust it has already earned among its customers. This is where the future of the Admin PKI lies, in terms of both its market potential and its financing.

The **FOITT's response** to the recommendations made by the SFAO in this report is stated after each recommendation. The **Finance Delegation** took cognisance of the SFAO's report at its fifth session held in August 2007.