EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
CONTROLLA FEDERALA DA FINANZAS

Federal Office of Information Technology, Systems and Telecommunication

Does the Admin PKI correspond to the original objectives and the needs of the Federal Administration and the Cantons?

Original text in German

11 June 2007

Contents

List of abbreviations

CA	Certification Authority
CPA	Cost and performance accounting
CSP	Certification Service Provider
DTS	Digital Tachograph System (a FEDRO project)
e-dec	Electronic customs declaration
e-Gov	Electronic Government
e-pass	Swiss passport containing computer-legible information such as passport photo, fingerprints, etc.; a certificate is used to prevent falsification
FDJP	Federal Department of Justice and Police
FITC	Federal IT Council
FOITT	Federal Office of Information Technology, Systems and Telecommunication
FSUIT	Federal Strategy Unit for IT
LRA	Local Registration Authority
NAM	New Accounting Model for cost and performance accounting in the Federal Administration
PKI	Public Key Infrastructure
RA	Registration Authority
ROI	Return on investment
SCMS	Smart Card Management System
SFAO	Swiss Federal Audit Office
SITC	Swiss Information Technology Conference
SSO Portal	Single Sign-On Portal for centralised authentication of external users (mainly from the Cantons) of FDJP applications
ZertES	Swiss federal law on the electronic signature

1 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.

2 Mandate and audit performance

2.1 Mandate

On the basis of Articles 6 and 8 of the Federal Act on the Swiss Federal Audit Office (Federal Auditing Act; SR 614.0), the SFAO conducted an audit examination on the Admin PKI in April 2007. The examination mandate was to determine whether the development and operation of the Admin PKI correspond to the original objectives and the needs of the Federal Administration and the Cantons.

Accordingly, the key points of the examination were to:

- outline the history of the project since 2001 with the main decisions taken
- assess the present state of development, implementation and current operation
- assess the previous and future costs as to their profitability
- obtain the the status of KPMG certification
- assess the current and future needs of partners (Cantons) and customers and gauge the degree of customer satisfaction

The assessments were to be based on the project documentation from 2001 and the financial data available up to the time of the audit.

2.2 Legal basis

- Federal Act on the Swiss Federal Audit Office of 28 June 1967 (as at 20 July 1999) (SR 614.0)
- Federal Act on the Swiss Federal Budget of 7 October 2005 (Federal Budget Act, SR 611.0)
- Federal Budget Ordinance of 5 April 2006 (SR 611.01)
- Federal Act on Certification Services in the domain of the Electronic Signature (Federal Electronic Signature Act, ZertES, SR 943.03)
- Ordinance on Certification Services in the domain of the Electronic Signature (VZertES, SR 943.032)
- Technical and administrative regulations on certification services in the domain of the electronic signature (SR 943.032.1 / Annex)
- FDF Ordinance on electronically transmitted data and information (EIDI-V, SR 641.201.1)
- Ordinance on IT and Telecommunications in the Federal Administration of 26 September 2003 (Federal IT Ordinance, SR 172.010.58)

2.3 Audit scope and principles

The examination was conducted by IT auditors Peter Bürki, Stefan Wagner and Cornelia Simmen (audit lead). To fulfil the mandate, the large body of documentation was inspected and interviews were held with the individuals at the FOITT responsible for the various sub-projects and with various other bodies involved (FSUIT, SITC, the Cantons of Aargau and Zurich, GS FDF). Details on the form and scope of the inspections made are given in the working papers.

2.4 Documents and information furnished

All persons contacted in this respect provided the information required in an open and efficient fashion. The requested documents, some of which were quite substantial in size, were placed at the audit team's disposal quickly and completely.

2.5 Prioritisation of the SFAO's recommendations

According to the examination mandate, the SFAO grades the importance of recommendations and comments by priority (1 = high, 2 = medium, 3 = low). This takes account of the **risk** [e.g. extent of financial impact or significance of the observation; probability of damage being incurred; frequency of the deficiency (individual case, several cases, general) and recurrences; etc.] as well as the **urgency of implementation** (short term, medium term, long term).

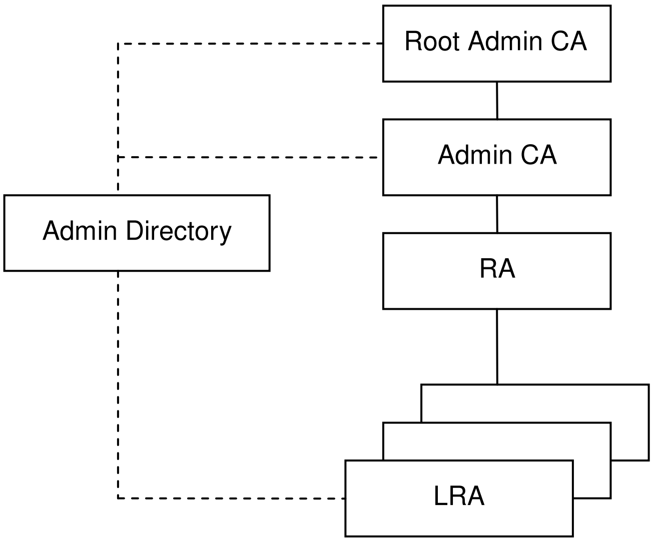
3 Introduction

As IT components become increasingly networked, an ever-expanding volume of data is being transmitted electronically. For legally binding transactions, users want to be certain that the data they receive (such as an e-mail, order, confirmation, etc.) really does originate from the assumed sender, that the content has not been tampered with while sending or saving, and that the transmission can be retraced. To meet so many security requirements, a multitude of rules and regulations are necessary, i.e.:

- legislative measures (laws, ordinances) governing the legal equivalence of electronic and paper-based correspondence;
- organisational measures ensuring the processes providing for traceability of transmission – comparable with sending a registered letter by post – and creating the prerequisites for authorised execution of all actions in this respect;
- technical measures – recognised as national and international standards – allowing for user identification and tamper-proof transmission.

Terms such as Public Key Infrastructure (PKI), Certification Authority (CA), digital certificates, authentication, signatures and encryption are directly connected to these legal, electronic and organisational measures.

Public Key Infrastructure (PKI) refers to all the processes, architectures, servers, workstations and software required for issuing certificates. A PKI infrastructure is hierarchically structured and consists of the following main components:



- The **Root Admin Certification Authority** (CA) is responsible for validating and logging the issuing of digital certificates, i.e. monitoring the Admin CA
- The **Admin CA** of the FOITT is responsible for issuing, managing and publishing digital certificates
- The **Registration Authority** (RA) of the FOITT manages the certificate applications
- The decentralised **Local Registration Authority** (LRA) is responsible for identifying the applicants for certificates, generating key pairs and transmitting these to smart cards.
- The **Admin Directory** is obliged to store and publish all authorised and revoked certificates.

The need to use **certificates** depends on the security requirements of the individual application. Different fields have different requirements in terms of authentication, signatures and encryption, either individually or in combination with each other. Certificates may be hardware-based (e.g. a smart card or token) or software-based (soft certificates). Not unlike a Swiss passport, a certificate constitutes a moral claim as to the credibility of the issuer and a technical one as to security, i.e. unforgeability.

Four categories of certificates are defined within the Federal Administration:

- **Class D**, medium grade/quality, for the secure authentication of individuals or computers, a soft certificate, used for e.g. access by external networks to applications within the federal network
- **Class C**, medium grade/quality, enables secure authentication, encryption and signature, a soft certificate, used for e.g. encrypting e-mails (secure messaging) within the Federal Administration
- **Class B**, very high grade/quality, enables highly secure authentication, encryption and signature, a personalised certificate on a smart card, issued only upon presentation of personal ID together with a valid passport or ID card
- **Class A**, very high, legally regulated quality requirements, qualified electronic signature equivalent to a handwritten legally-binding signature, cf. Chapter 5.6.

To meet specific requirements in terms of authentication, encryption and signatures, the FOITT can provide special customised certificates based on these predefined classes.

4 History of the Admin PKI

In January 1999, after taking note of the report “Setting up a certification infrastructure for the Federal Administration”, the Federal Council issued the mandate to set up a certification infrastructure for the Federal Administration. It commissioned the DETEC to coordinate the work, the FDF to draft the technical fundamentals, and the FDJP to prepare the binding force of electronic signatures.

4.1 Coordination and technical fundamentals

No observations could be made on the coordination tasks of the DETEC as the dossiers inspected did not contain any documentation in this respect; in any case, this was not the objective of the present audit.

Based on the initial project estimate of CHF 3 to 5 million, a WTO invitation to tender was issued in 1999 for the Secure Messaging project (SOGC No. 123, 29 June 1999). By the time the project was launched in 2000, the decision had been made in favour of a secure e-mail solution throughout the Federal Administration. This was based on certificates from Swisskey, a company that would subsequently discontinue all services a year later, right in the middle of the project. Thus, if the Secure Messaging project was to be continued, the FOITT had to decide in 2001 whether to use certificates from foreign providers or to venture into the issuing of certificates itself. The in-house option was chosen and, by the end of 2001, the FOITT had a functioning Admin PKI (generating, publishing and managing its own certificates) with its own dedicated, secure premises. Nonetheless, the Secure Messaging project remained in the pilot phase, as the solution chosen at the time failed to catch on and, consequently, not enough certificates were generated.

Further obstacles made their appearance in 2002. On the one hand, the Federal Strategy Unit for IT (FSUIT) was opposing the creation of an in-house federal CA (claiming there was no need within the Federal Administration or the Cantons, this was not the core task of the Confederation, and that certificates could be purchased) even though the FOITT had received a Federal Council mandate to issue certificates. On the other hand, the FOITT was convinced that a single hardware-based solution with certificates for authentication, encryption and signatures was the only way forward for all security requirements. As a result, other PKI projects launched between 2001 and 2004 made very little headway, and the Cantons started looking for their own solutions for acquiring certificates.

2003 saw the invitation to tender and implementation of the current Class B certificates. The procurement of a Smart Card Management System (SCMS) was halted, as the volume of certificates issued was simply too low. In August of the same year, the FITC agreed in principle to a sole Admin PKI operated by the FOITT. In October and December respectively, it was decided that the services of the then Admin PKI for Classes 2 and 3 (now Classes B and C) could also be offered to the Cantons, However, it was never explicitly defined at the time who would be responsible for previous and future investments and operating. The expenses for the Admin PKI cannot be traced in the state accounts until 2004. In retrospect, it must be said that it was only the FOITT’s perseverance that prevented the Admin PKI project (which had already run up investments of over CHF 2 million) from running aground.

In 2004 the FSUIT conducted a survey on the need for certificates in the Federal Administration and the Cantons. The findings resulted in the FSUIT "officially" commissioning the FOITT, in a decision on 24 May 2004, to operate the Admin PKI for the issue of Class B, C and D certificates as a shared service using cross charges. One of the outcomes of this decision was that the solutions that had been launched in the meantime by other bodies (e.g. the Canton of Zurich) could be compared with those of the Admin PKI.

The FOITT's reorganisation project ("*Change BIT*") in 2005 reassigned the responsibilities with respect to the Admin PKI. The FOITT was aware at the time of the opportunities posed by projects such as e-pass, DTS and SSO Portal. Thanks to a vastly improved communication system and the expansion of the PKI team, the Admin PKI project was slowly but surely ramped up again. The FITC gave the FOITT the go-ahead to seek KPMG certification to also issue ZertES-compliant Class A certificates, provided that such certificates would not be financed with cross charges.

The Admin PKI then really took off in 2006 with the rollout of some 25,000 Class B certificates for the FDJP's SSO Portal, resulting in widespread recognition of the FOITT solution among the Cantons. This experience made a significant contribution to the PKI team's level of know-how within the FOITT. Despite some hiccups encountered in the practical testing phase, overall it was regarded as a success. Based on this success and the experience thereby gained, the "Relaunch Secure Messaging (RSM)" and "Smart Card Management System (SCMS)" projects were reactivated.

Following an FITC ruling, FOITT applied for KPMG certification for its Class A certificates in 2006. The issuing of certificates was never the primary objective here: what the FOITT really wanted was to obtain a nationally and internationally recognised seal of approval attesting to the trustworthiness of the entire Admin PKI, and thus also of the FOITT itself.

The future development of the certificate market will tell whether the Admin PKI can hold its ground and the extent to which it will be influenced by the private sector.

4.2 Legal framework

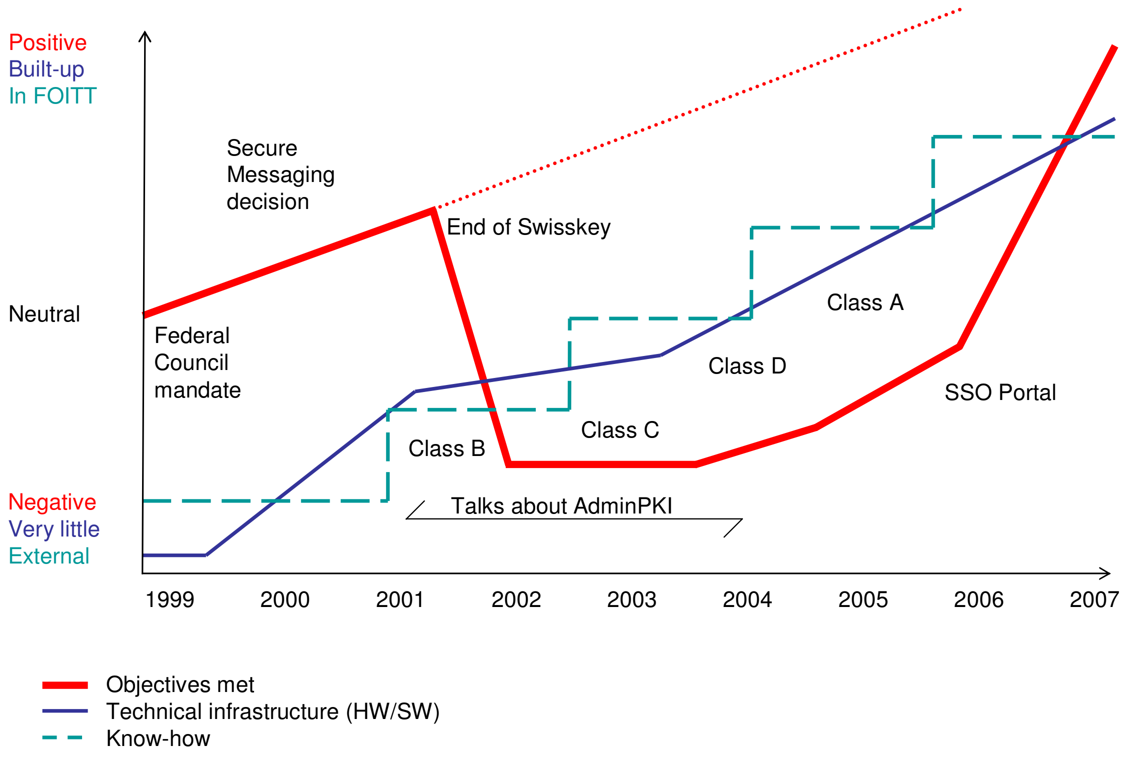
In general, the legislative requirements were regarded as being met. It is generally recognised that electronically signed documents are now legally equivalent to paper documents, provided that they meet certain conditions laid down by law. The relevant laws and ordinances were adapted and submitted for debate and have now been in force for a number of years.

4.3 Graphic overview of milestones

The **red** line shows the extent to which the objective has been met. As the chart shows, the original mandate from the Federal Council progressed according to plan until the demise of Swisskey had a sudden and disastrous effect on the project. Things started to pick up slowly but surely with the implementation of Classes B, C and D, and then quite dramatically with deployment of the SSO Portal.

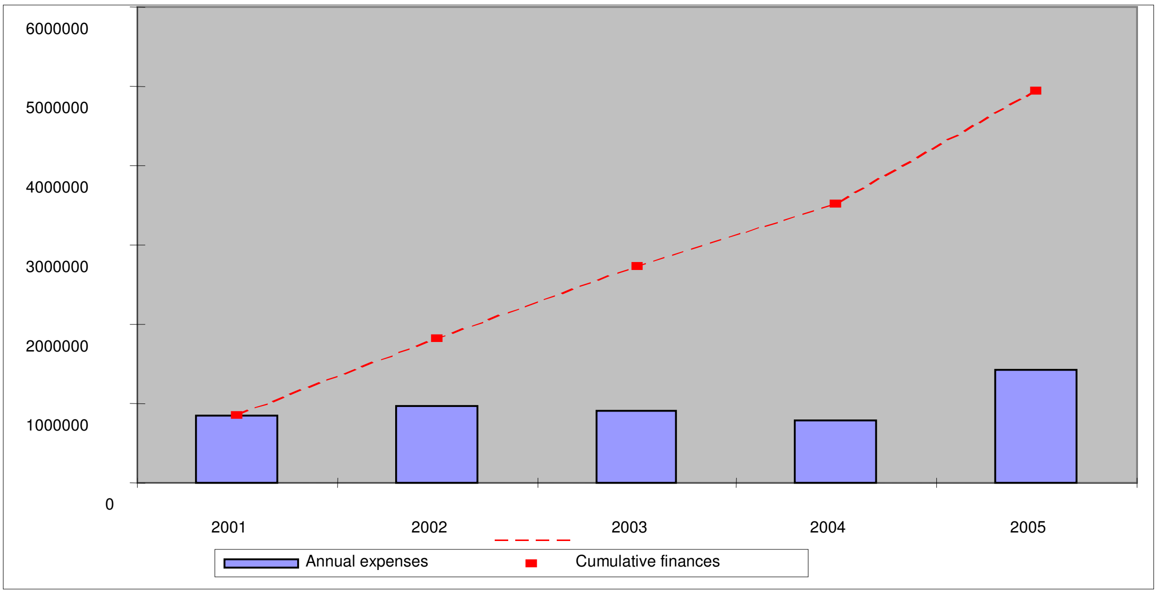
The **blue** line shows the development of the technical infrastructure (hardware and software).

The **green** line shows the know-how acquired in setting up the infrastructure and the experience gained.



4.4 Graphic overview of finances

This chart is based on the SFAO's compilation of the invoices inspected. It refers only to external costs and does not claim to be exhaustive.



5 Present scenario

5.1 Current status of the project

As evident in its history, the Admin PKI has had to overcome many obstacles before asserting itself. In retrospect, a lot of valuable time was lost and much funding irretrievably spent. This was not all the fault of the FOITT, however: in the years from 2001 to 2004, neither the Federal Administration nor the Swiss market was really ready for widespread use of digital certificates. In fact, the lack of demand for certificates was what brought down companies like Swisskey. At that time, the advantages and possibilities of digital certificates were not sufficiently known and appreciated.

The decision by the FDJP to create a Single Sign-On Portal, for secure authentication of all users of the department's special applications, gave the Admin PKI new impetus and a fresh start. In a last-ditch attempt, the FOITT rose to the challenge in 2005, breathing new life into the current Admin PKI with a reformed project team. The rollout of over 20,000 Class B certificates within one year made great demands on all those involved. It was, however, something of a cold shower, looking at some of the unsatisfactory customer feedback encountered in the early stages.

In the end, however, the current team managed to revive the Admin PKI and – despite some teething troubles – passed the final test with flying colours. What's more, some new and valuable experience was also gained along the way. Today, although the FOITT product catalogue defines a range of standard certificate classes, these configurations are no longer set in stone. More and more certificates are now being developed and issued on an application-specific basis, as the PKI team now has the know-how to respond individually and optimally to its customers' requests. At http://www.bit.admin.ch/adminpki/, interested customers can view product descriptions as well as a range of other publications, such as guidelines, standards, checklists, etc. Substantial progress has also been made in this field.

A PKI will never be a complete, self-contained infrastructure, so there is always bound to be both positive and negative customer feedback. Technical innovations, modifications and expansions are required all the time. However, the audit team received a lot of positive feedback on the Admin PKI and thus has a favourable opinion of the project as it stands today. The FOITT has proven that its hard work is now finding acceptance even beyond the Federal Administration. Of course, there are still some weak points to be improved and/or eliminated. However, overall, the FOITT has built up a solid foundation for further development and a good chance of becoming one of Switzerland's leading Certification Service Providers in the future.

5.2 The Cantons

The use of digital certificates for accessing Federal Administration applications has been a matter for discussion for several years now between the Cantons and the FOITT. Various surveys conducted by both the Swiss Information Technology Conference (SITC) and the Federal Strategy Unit for IT (FSUIT) show substantial discrepancies in the need for digital certificates. Prior to the audit, the audit team sent a short questionnaire to the Cantons of Zurich and Aargau to enquire about the current status and development of certificate requirements.

When the FOITT project faltered between 2001 and 2004, this resulted in the Canton of Zurich setting up its own PKI; there was also talk of teaming up with Swisscom for certificates. In the end, the decision was taken in favour of the Admin PKI. The Canton of Aargau says that the Admin PKI was its preferred solution right from the start. In general, the technical solution is found to be satisfactory. However, at least one Canton still has issues with the organisational setup, nothing that could not be resolved by the FOITT though.

There is no disputing that the use of hardware-based certificates met with some initial resistance among the Cantons. It represented a huge cost factor for the Cantons and associated bodies, entailing the implementation of the organisational processes needed and the procurement of the technical infrastructure. What's more, the FOITT was not always able to deliver on time and, as the correspondence shows, the response and delivery times were found to be unacceptable. The rollout of the SSO Portal brought a change of fortune for the FOITT, however. Since then, the criticism has died down and, according to the SITC, most Cantons are now satisfied with the FOITT offering. Statistics show that, as of mid-April 2007, 24,000 of the 26,580 Class B certificates issued were in use in the Cantons. Several Cantons now realise that they can also use these certificates for securing their own applications, and the corresponding projects are already underway (e.g. talks between the FOITT and *Verwaltungsrechenzentrum AG St. Gallen* on the use of certificates). However, these will not generate any additional revenues for the FOITT.

Through the use of Local Registration Authorities (LRA) in the Cantons, but also within the Confederation, the process of issuing certificates has been brought closer to the end-customer. An LRA (of which there are some 80 in use at present) forms an important element in the overall security system of a PKI. Correspondingly, these must operate according to strict guidelines drawn up by the FOITT. An audit conducted in 2005 on several LRAs on behalf of the FOITT highlighted some of the weak points that existed. These were reviewed by the FOITT and, over time, most (though not all) have been eliminated. However, it has not yet been defined who will be responsible for monitoring the LRAs.

Recommendation 5.2 (Priority: 1)
As the LRAs form an important element within the overall security process of issuing certificates, regular audits must be conducted to ensure that these bodies meet the requirements laid down. As the product provider, the FOITT must ensure that such audits are conducted and that the corresponding requirements are decreed by the FITC.

The FOITT will draw up an audit plan for LRAs by the end of the year and then submit a proposal for the corresponding requirements to the FITC.

5.3 Competition

After Swisskey collapsed, there were no Swiss providers of certificates for quite some time. It was only after the signature law (ZertES) came into effect that there was a legally defined basis under Swiss law to seek a solution with recognised standards. Despite a huge consultant market in Switzerland, there are only three recognised providers of ZertES-compliant certificates. Many consultant firms use either proprietary certificates or those of leading international providers such as Verisign, Cybertrust, Symantec, etc. For eGovernment solutions, the standards are high with regard to the credibility and reliability (continuity) of a CA. With foreign providers or those not certified as being ZertES-compliant, these standards are not met – at least, not entirely.

Obtaining KPMG certification will open up some very interesting prospects for the FOITT. The FOITT has already entered into an agreement with Swiss Post and tested the technical implementation to extend the use of electronically registered post (IncaMail) to Federal Administration staff, using cross certification. This is an example of how the public sector can be served with FOITT certificates and the private sector or individuals with Swiss Post certificates, thus enabling an implementation of eGovernment services to a wide public.

Swisscom and Quo Vadis will not pose any competition to the public sector for the foreseeable future as the markets these serve are smaller and more specific. There are not yet any products using large volumes of Swisscom-issued certificates. Neither are there any products in the public domain that would foretell the breakthrough of Swisscom certificates on the narrow Swiss market. Nonetheless, a joint project with the FOITT, like the one with Swiss Post, could well be an interesting option for Swisscom.

For Swiss Post and Swisscom, and also for the FOITT, the economic viability of their PKI cannot be calculated on the basis of the price of individual certificates. The primary benefit lies in the potential for securing in a simple manner the data and applications of a large number of users from different organisations. In any case, the main party to benefit is the customer, whether the certificates originate from Swiss Post, Swisscom or the FOITT.

The commercial international providers can and will continue to offer and sell low-grade certificates or those with a special system constellation. When high quality standards are required, however, no alternatives have been available in Switzerland until now, a fact that augurs well for the FOITT.

5.4 Ongoing projects

The Admin PKI is a basic product used for issuing certificates. The corresponding project to create the initial infrastructure was officially completed, i.e. put into official operation, in 2002. New customer requirements have continued to emerge since then and will continue to do so in the future. The FOITT's offering, originally limited to secure messaging, has gradually been expanded and the new findings correspondingly improved. For each expansion of the original basic infrastructure, additional separate projects were and will be launched and charged. Such projects in the past were: the development of PKI Class 2 (today Class B), the introduction of the PKI in the Cantons in association with the FDJP's SSO Portal, the development of Classes C and D, the expansion of the infrastructure to CA3 and the issuing of certificates for the Digital Tachograph System (DTS). Secure messaging, Class A certification and the Smart Card Management System (SCMS) are each currently the subject of separate projects. These lists are not exhaustive but do serve to illustrate the variety and scope of problems encountered in association with the Admin PKI.

The audit team inspected all past project documents, i.e. offers, contracts and invoices. The documents are clearly filed and, in general, the cash flow was traceable, based on the contracts and also, from 2006 on, extracts from SAP. However, no inspections were made with respect to completeness or procurement. The compilation of all invoices inspected serves primarily to evaluate the expenses incurred to date, in accordance with Chapter 5.5.

5.5 Investments, budget

As the preceding chapters have shown, the FOITT's decision to set up its own CA was one that was taken out of necessity. In doing so, it opted to keep a key security-relevant function within the Federal Administration rather than leaving it to an external provider. When it comes to selecting a suitable CA, it is important to be able to trust in its serious nature as well as its continued existence on the market. A high degree of security must be met, depending on the requirements of the certificate. So, in such cases, is it better to entrust this security service to an in-house provider within the Confederation or outsource it? At this stage, the question of whether or not it was right to opt for hardware-based certificates is no longer relevant. The FOITT has long since recognised that the market needs more than just a single, inflexible hardware-based certificate.

The FDJP's decision to use smart cards for the SSO Portal, however, set the course for future developments. Either the dormant Admin PKI project would have to be revived and started up again, to meet the needs of the FDJP and those of the Cantons, or another Certification Authority would have to be found on the open market. The latter solution would inevitably have led to the "grounding" of the Admin PKI with all sunk costs having to be written off. The rulings of the Federal IT Council (FITC) thus came just in time and included an important factor: a functioning PKI can only be operated after the appropriate infrastructure and know-how are put in place. The investments needed to do this should not be underestimated. If such expenses were to be recovered through the sale of certificates, the certificates would have to be sold at a price that no customer would ever realistically pay. The FOITT's price policy is comparable to that of Swisscom or Swiss Post and can be said to be competitive, even quite reasonable. In principle, however, the issuing and management of certificates should be self-sustaining. The breakeven point for the cost of current operation can only be reached by issuing, according to FOITT calculations, between 100,000 and 130,000 certificates. Such assumptions are only realistic if certificates are to be used as a security element in other Federal Administration applications.

The audit team combined all the invoices, based on the documents placed at their disposal. The totals calculated were then compared with the figures from the product manager. The expenses for the years 2001-2003 could not be completely traced on the basis of SAP. The years 2004 and 2005, however, tally almost perfectly, taking account of accruals. Bookings have become increasingly precise since 2003, i.e. the Admin PKI is charged not only external costs but also internal FOITT costs on a pro rata basis. In addition, as of 2005, the booked or apportioned costs are evaluated and interpreted by the product manager, resulting in costs that are somewhat more precise.

The SFAO’s compilation shows an overall total of some CHF 5 million in external costs, i.e. payments made to suppliers and service providers, for the years 2001-2005. This amount contains not only operating expenses, including maintenance and licences, but also all projects started in association with the issuing of certificates, e.g. development of the infrastructure for Class 2 (today Class B), Classes C and D, setting up registration for the Cantons, etc.). Assuming (based on estimates made by the then and current project managers) the number of PKI employees in each case – two in 2001/02, four in 2003/04, six in 2005/06 – with assumed average expenses of CHF 200,000 per employee and year, this amounts to CHF 4.8 million in internal costs run up to date.

Revenues posted for the years 2001-2005 are not sufficiently transparent and meaningful to be evaluated by the audit team. A comprehensive absorption costing system can only really be put in place from 2007 on. The budgeted figures according to the NAM guidelines provide for operating expenses for the Admin PKI of some CHF 3.65 million, with an anticipated revenue, including cross charges, of some CHF 2.8 million (of which CHF 700,000 in income having a financial impact), corresponding to a budgeted loss of CHF 850,000. This does not include CHF 1 million in ongoing projects. The estimated income/expenses for the years 2008-2011 show an increasing “profit” from 2009 on, provided that the number of certificates issued can be grown as assumed and costs can be contained within the given limits. Although it is very difficult to evaluate these figures at this stage, the audit team is optimistic of their being attained.

A fair profitability analysis cannot be carried out under the aspects previously mentioned. The benefit of a PKI is only generated indirectly through the simplified safeguarding of applications. The eGovernment partners involved are the main players to benefit from the savings potential. However, the potential synergies to be generated are further enhanced through the active cooperation with Swiss Post. Based on experience to date, it must be assumed that the investments made of some CHF 12 million cannot be directly recovered and should be regarded as start-up costs to be written off. These facts, or more specifically, the differentiation between the investments needed and actual operation, which should be based on economic criteria, must also be taken into account in the calculation guidelines. In accordance with the principles applicable to calculating transfer prices, services provided within the Confederation may only be charged on the basis of the budgeted full costs, i.e. profit or risk must not be included. This price policy is only partially traceable in the investments posted and the annual cross charges made, particularly when costs are passed on outside of the Federal Administration, e.g. to the Cantons. Full-cost coverage is only possible if no additional funds (cross charges) are needed to finance a product. The investments made are not included or recovered in this calculation.

The audit team concluded by observing that the creation of the Admin PKI and the issuing of certificates have produced a business that cannot simply be abandoned from one day to the next. At the very least, a successor system would have to be found for valid certificates still in circulation, entailing financial consequences for the FOITT.

Recommendation 5.5 (Priority: 2)
In setting the prices for the various certificates, it must be taken into account that full-cost charging is not attained until there is no more cross charging. Investigations should therefore be made to see if the prices charged outside of the Confederation could be different, i.e. higher, than those within the Federal Administration, to enable full-cost coverage within a short period of time.

The FOITT will examine its cost allocation and pricing and discuss with the FFA the charging of higher prices outside of the Confederation.

5.6 ZertES

In the decision of 27 June 2005, the FITC authorised the FOITT to offer Class A certificates within the Federal Administration. At the same time, it was decided that this service could not, like Classes B-D, be financed with cross charging, but that the certificates should be charged at full cost. On this basis, the FOITT received the go-ahead to introduce certification as provided for under the ZertES. In a preliminary audit in autumn 2005, KPMG – the only accredited certification body in Switzerland – determined the extent to which the FOITT would meet the certification requirements. Following the announcement of the results, the mandate was issued on 31 May 2006 to conduct the certification audit. Between August 2006 and February 2007, KPMG audited the business organisation and operation processes within the FOITT and the logical infrastructure of the Certification Service Provider (CSP). The resulting audit report was presented in early April 2007.

The audit found that the processes and infrastructure do not yet meet in all areas the very high security standards laid down by law. However, there were no deficiencies that could not be resolved within the deadlines set by KPMG. It can thus be assumed that the FOITT will obtain its certification during the second quarter of 2007. The sale of Class A certificates is not the primary aim of certification, however. Realistically speaking, this remains a very small market: there are, as yet, no concrete requirements within the Federal Administration, and even the private sector is showing a certain degree of hesitation.

Rather, the main objective in getting the FOITT officially recognised as a CSP is to help build its reputation of trust, given the strict legal basis and standards on which certification is granted. To understand this objective more clearly, it must be pointed out that the processes and infrastructures audited by KPMG are the same as those used accordingly in issuing all other certificates. The added value that the FOITT gains in providing/issuing certificates should be reflected in the volume of certificates sold overall, which, in turn, would improve the financial situation. This also emanates from the cost/benefit analysis for the ZertES project. Together with a modest income from the sale of Class A certificates, the “revenue” in the form of quantifiable benefit is estimated at a likely sum of CHF 450,000. Deducted from this theoretical value are annual operating costs and interest of some CHF 230,000. The ROI would thus be reached within five years. The audit team views the FOITT's calculations as realistic, in principle, though not cost-effective / profitable. Rather, certification has a strategic and political background that should also be taken into account in the equation.

As, according to the FITC ruling, Class A certificates may not be funded using cross charges, a separate project called “Admin PKI recognition for Class A” will be run until certification, with the associated external costs posted at around CHF 1.1 million.

In future budgets, the costs and income associated with the above scenario must continue to be posted separately and may not be listed under the global “PKI costs & income” budget or set off via the Admin PKI accounts. To ensure that the FITC ruling can be observed, the costs and income must be posted transparently at all times.

Recommendation 5.6 (Priority: 1)
All costs and income (operating costs, investments, repeat audit, sales income, etc.) associated with the Class A certificate must be budgeted and accounted for separately. The guidelines in the FITC ruling of 27 June 2005, under which there must be no combining with Classes B-D (cross charges), must absolutely be observed by the FOITT.

The FOITT will post the costs and income associated with the Class A certificate separately each year. Because, in practice, Class A and B certificates share the same infrastructure and operating processes (as is also the case for other CSPs), this reporting is to be based on model calculations.

6 Outlook and appraisal

During the past few years, the FOITT has successfully built up both the infrastructure and the know-how required to meet customers’ requirements for certificates of different grades and qualities, covering application-specific security aspects. With the rollout of some 25,000 certificates for users of the SSO Portal in 2006, the FOITT proved its ability to issue large volumes of functioning certificates on a time-critical basis. With its ongoing CSP certification by KPMG, the FOITT also demonstrates the quality and security of the infrastructure and processes used to issue ZertES-compliant Class A certificates. The FOITT will probably be the fourth provider on the Swiss market authorised to offer this type of certificate. As the infrastructure and processes for Class A are the same as those used for issuing all certificate classes at FOITT, the public sector now has the means to implement eGovernment solutions at a very high security level.

Once the FOITT obtains KPMG accreditation, it will have met an important prerequisite as a credible and trustworthy CA on the narrow Swiss market. This may become an important federal task. KPMG conducts a repeat audit of the high standards each year, ensuring consistently high quality. The FOITT's certification can also be regarded as important in that already over 40,000 certificates, of which 65% are Class B, are in use. Although Swiss Post and Swisscom have been certified for some time now, they did not start offering their products until after certification so they have not yet gained the practical experience of large-scale rollouts. The FOITT has signed a "roaming" agreement with Swiss Post with respect to IncaMail – the sending of electronically registered letters – thereby generating potential synergies in the private sector too.

Issuing certificates only makes economic sense if enough of them can be sold. Class B to D certificates will thus form a key success factor. At present, it seems rather unlikely that the sale of ZertES-compliant Class A certificates could become a self-sustaining business. Only in very few cases does the Swiss Code of Obligations require a qualified written form for legal transactions, and few of these are expected to be conducted electronically in the future. KPMG certification must therefore be regarded primarily as a seal of quality not just for the issuing of certificates but also for the FOITT itself. The main objective lies in obtaining the customers' trust in the processes and technical operation. The FOITT can use this opportunity to secure a potentially large number of applications through the possibilities opened up by digital certificates.