Information Paper

How much do you pay for your PKI solution?

A closer look into the real costs associated with building and running your own Public Key Infrastructure and 3SKey.

This study has been conducted in cooperation with SEALWeb, an independent and trusted consultancy firm who has proven experience in managing PKI projects in the financial services and other industry sectors. The case study figures are representative of the average time and budget that customers of SEALWeb typically spend on PKI implementations.

Total Cost of Ownership (TCO)

Understanding and calculating all the costs related to a PKI solution

Contents

Introduction

In the world of electronic banking, proof of identity is often very complex, involving numerous tokens, passwords and access cards for a single transaction. The use of Public Key Infrastructure (PKI) and adoption of electronic signatures are now considered best-in-class for securing banking communications. PKI enables both financial institutions and their customers to ensure that instructions are authentic, unaltered and legally binding.

Implementing a cutting edge PKI infrastructure is costly and often complex to build and maintain. It requires for you not only to invest in the infrastructure and build expertise but also to permanently upgrade the changing technology and evolve with new security threats. Therefore, enabling strong authentication and digital signatures with your customers is not only a question of 'keys' and 'tokens'.

Most 'financial' decisions for a PKI solution are based on a comparison of the most obvious costs, therefore overlooking the hidden, and often more expensive costs.

TCO or Total Cost of Ownership allows you to understand and calculate all the costs related to a product or service. It includes not only the direct and most visible costs of a solution, but also unveils the often hidden indirect costs for building and maintaining the solution. In the world of PKI, the TCO includes the more visible charges such as infrastructure investments, cost of developing the applications, product licenses, installation and training, etc… and the often hidden recurring charges to run and maintain the service. The latter is not always easy to identify and not obvious to calculate.

SWIFT, together with SEALWeb, conducted a study comparing the costs for a financial institution to build and maintain a proprietary PKI with the costs of implementing 3SKey. The study revealed that institutions could reduce their cost up to 40% when using 3SKey.

This information paper describes the drivers to use PKI solutions, breaks down the different cost components to build and maintain such infrastructure, describes the implementation options for an organisation and reviews all the costs in three typical scenarios. This starts with a financial institution with limited needs up to a large organisation with extended requirements.

Public Key Infrastructure (PKI) - What is it and why?

What is PKI?

A Public Key Infrastructure or PKI is a system for the creation, storage and distribution of digital certificates. PKIs allow organisations and their customers to verify the authenticity of financial messages they receive. When transferring a financial message, the sender has a private encrypted key that needs to match the recipient's public key. Only when the two match can the recipient verify that the message is authentic (Fig. 1).

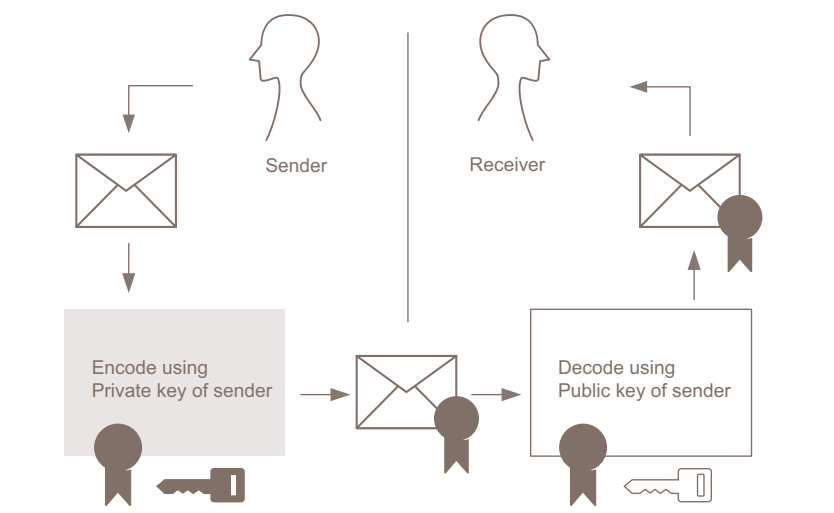
To implement this solution, an individual generates a private (secret) key locally, which will be used as a credential for signing purposes. For security purposes, such credentials are often stored on external devices, such as USB tokens or smartcards. A public key is created and linked to the individual's private key by a trusted party, also known as the Certification Authority or CA. The public key is used to authenticate the individual. Each key is a unique string of numbers. The CA can revoke a specific certificate; for instance, if its lifetime has expired or if there is concern with the certificate, such as theft of an associated private key that has been reported.

Certificates are associated with identities, for example with the name of a person or a function within the organisation. This is the role of the Registration Authority, also known as RA. The RA is responsible for the registration and controlling the identity of its users. Therefore, they will apply their Know Your Customer policies (KYC) and security processes prior to linking the identity of the user with a certificate. Users sign their financial instructions, such as a payment by using their private key. The financial institution verifies the signature by using the associated certificate and will check the validity of this certificate with the CA (e.g. whether the certificate has been revoked).

Why use PKI?

There are three main advantages and differentiators of using a PKI solution over any other electronic identity means:

1. **Checking the authenticity of the sender:** Authentication means verifying the identity of the person who sent and signed the data and being sure that they are the person who they say they are. PKI facilitates remote authentication between parties, assuring the receiving entity that the information originated from the sender who owns and has protected access to his or her private key.



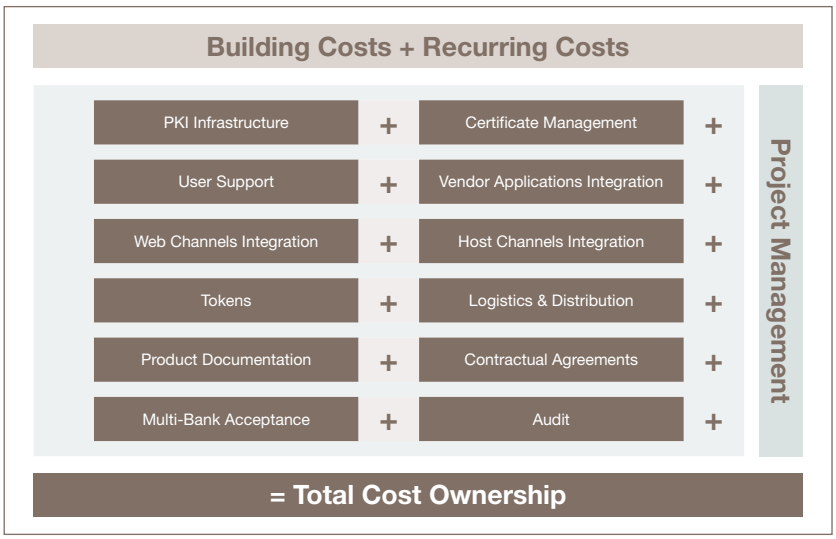
(Fig. 1) Basics of a PKI solution

2. **Controlling the integrity of the signed information:** Integrity means ensuring that data cannot be corrupted or modified, i.e. a transaction can therefore not be altered. With PKI, the content of the exchanged data is guaranteed by its electronic signature. If the data is modified afterwards, then the signature will no longer be valid.
3. **Proof of sender:** Non repudiation means ensuring that an action cannot be denied after a given event. With PKI, the receiver can prove that the data could only have been signed by the owner of the private key. This is becoming increasingly important for audit and legal purposes.

Cost components of a PKI solution

It is mostly easy to identify the direct costs such as expenses related to software, licenses, hardware, etc… to build and run a PKI solution. However, these are only part of the Total Cost of Ownership or TCO. To build and maintain a PKI solution, there are many different cost components to consider.

The diagram below (Fig. 2) provides an overview of the typical investments needed to run a successful PKI project. Each of the components represents an initial investment to build the solution and later a recurring annual running or maintenance cost.



(Fig. 2) Cost components of a PKI service

Common implementation options and 3SKey

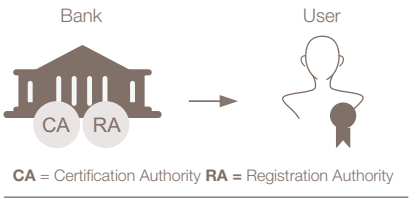
Institutions planning to implement or replace a PKI solution have different options available. Each of the implementation strategies have different costs and benefits and the decision will likely be driven by factors such as:

- Number of users
- Budget allocation
- Need for tailored interfaces and workflows or standard PKI services
- In-house knowledge and expertise of PKI
- Customer support needs
- Secure premises
- Need for multi-bank acceptance
- Vendor integration of your security solution

Therefore, an institution will have to make a choice between using a third party PKI provider to delegate the certification of the users, build and run an in-house PKI infrastructure or use 3SKey.

Building and running an in-house PKI-infrastructure

If an institution chooses to build and manage its PKI solution itself, it controls the full PKI architecture. The solution can be customised to the specific business needs including the identification of an appropriate security device for its users. The choice to build an in-house system depends on multiple factors such as the experience of the organisation with PKI, the number of customers to serve and the existence of an internal security framework that can be reused.



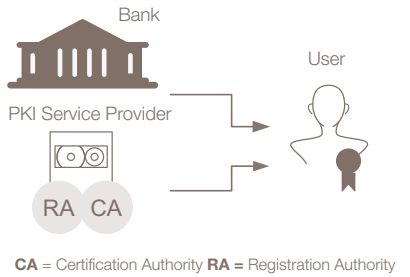
(Fig. 3) In-house PKI

The institution manages the acquisition of the required hardware and software components to enable the generation of digital certificates. Digital signatures and authentication mechanisms need to be integrated in internal applications. A regular audit of the infrastructure has to be conducted by the organisation itself. Also, internal and external support has to be planned to assist users with the installation and use of the digital certificates, help application software vendors during the integration, and support internal development teams.

This choice is often the most expensive implementation option and can only be selected when a large volume of users use the PKI solution and the institution has a proven experience with security infrastructures and PKI.

Using a third party PKI provider

Instead of building its own solution, an institution can also go for a 'Managed PKI', outsourcing to a specialised PKI service provider. In such a scenario, the technology and infrastructure will be managed and hosted by a trusted third party. The PKI provider will certify the end-users prior to issuing the digital certificates towards the customer. The trusted PKI provider will usually already have in place a regular audit of the technology and infrastructure.



(Fig. 4) PKI Service Provider

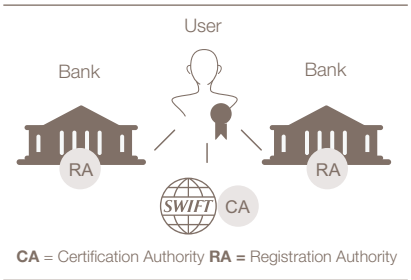
The institution needs to select the third party according to its business needs, the size of its customer base and also geographical scope. They will typically pay a one-time and recurring license fee for the use of the PKI infrastructure and also a one-time and recurring fee per user. The digital certificates will need to be integrated in the proprietary products and solutions of the institution, often with the assistance of the selected third party. The level of possible adaptation and customisation is mostly limited. The technical support for basic user queries will be handled by the organisation itself whilst the more complex problems will be escalated to the PKI provider.

On top of this, regardless of whether a third party or an in-house solution is used, other cost elements should not be overseen. These include amongst others project management, the organisation of regular audits, setup multi-bank acceptance when required, monitor threats and technology evolution and migration to a new security infrastructure (on average every five years).

Using 3SKey

Instead of building its own PKI or relying on a third party PKI provider, financial institutions can now also take advantage of the 3SKey service. 3SKey was designed to respond to a growing demand from financial institutions and their corporate clients for an international and interoperable digital identity solution. With 3SKey, SWIFT takes away the burden for a financial institution to develop and maintain the technical infrastructure and issues digital certificates, whilst for their customers it allows them to manage the users and tokens by using a secured web portal. This model offers users a single certificate solution, which they can use with many different financial institutions and over any channel.

Each financial institution will register its users independently by applying their own registration and KYC procedures, and subsequently associate the identity of the user with the 3SKey certificates. For financial institutions it offers a service that responds to their customer demand for a multi-bank solution. Thanks to a multi-registration model, financial institutions are not dependant on each other for checking the user identity. Moreover, 3SKey significantly reduces the investments and running expenses to manage an in-house PKI infrastructure or contracting with a third party PKI provider.



(Fig. 5) 3SKey

Financial institutions pay a one-time and annual service fee for using the 3SKey service within their banking group regardless of the number of users, channels and countries where they use the 3SKey certificates. This makes 3SKey a very flexible and scalable solution, suitable for small, medium-sized and large organisations.

To ease and speed-up the integration of 3SKey for financial institutions, their customers and within third party financial applications software, 3SKey has been built using common and widely used industry standards (e.g. RSA 2048 keys, X.509 digital certificates, …). Also, integration toolkits and APIs are made available to ease the project implementation. SWIFT provides ongoing support to financial institutions and the vendor community during the integration and use of the service, and also provides end-user assistance for the installation and activation of the 3SKey digital certificates.

Implementing 3SKey will allow organisations to offer a multi-bank solution to the user, whilst reducing TCO by using a cost-effective infrastructure operated by SWIFT, a trusted and neutral party.

Comparing the needs and benefits of different PKI implementation options

The table below summarises the benefits of each PKI implementation strategy and how the needs are addressed with each option (Fig. 6).

Benefit /Needs	In-house	PKI Provider	3SKey
Outsource infrastructure	⊘	✔	✔
Multi-bank acceptance	⊘	⊘	✔
Large geographical coverage	⊘	⊘	✔
Savings in technology renewal	⊘	✔	✔
Customisation of interfaces/workflows	✔	⊘	✔
Cost-effective scalability	⊘	⊘	✔

(Fig. 6) PKI Implementation comparison

Case Studies: Comparing the costs of a common PKI implementation and 3SKey

In order to conduct this study, typical scenarios have been identified. These different scenarios address the most commonly used models of PKI in a variety of financial institutions. The following variables were used to define the different case studies.

- Using a third party PKI versus building an in-house PKI infrastructure
- Size of the institution in terms of number of users
- Limited usage versus adoption of PKI across all platforms
- Need for multi-bank acceptance
- Number of user applications requiring integration

Three main scenarios have been chosen to compare typical configurations in financial institutions. In the respective case studies, the building and running costs were compared with 3SKey (Fig. 8).

$$TCO^{*} = \frac{\text{Cost to build the PKI} + \text{Price of tokens} + (\text{Annual service running costs}) \times 3 \text{ years}}{\text{Number of digital certificates}}$$

(*) Cost per user on a 3-year basis

- **Cost to build the PKI =** all investments and expenses associated to buy, develop and build the infrastructure and solution
- **Price of tokens =** the unit price paid for the tokens and associated services
- **Annual service running costs =** all recurring and maintenance fees associated with running and supporting the service
- **Three years =** the typical life cycle of a digital certificate and hardware security device before it must be renewed
- **Number of digital certificates =** the institution's number of users equipped with a digital certificate

(Fig. 7) Total Cost of Ownership (TCO) formula

For each case study, the average time and budget spent for all the cost components to build and run the service (as described in the section Cost components of a PKI infrastructure) were calculated based on experience and real costs of PKI implementation projects of a similar nature.

The cost for a similar implementation with 3SKey was then calculated taking into account the service and token fees, as well as the project and running costs for the components still managed by the institution itself.

To calculate the Total Cost of Ownership (TCO) of a self-managed PKI solution and compare with the costs of the 3SKey service, the formula in Fig. 7 was used providing a total cost per user.

The following section presents the three selected cases studies, a quantification of all the cost components and a comparison of the TCO per user with 3SKey.

1. Institution with small user base and limited needs	2. Institution with medium user base and regular needs	3. Institution with large user base and extended needs
— PKI outsourced to a third party — 1K - 10K users — File signing only — No need for multi-bank acceptance — 5 vendor applications	— PKI outsourced to a third party — 10K - 50K users — File signing and web-banking — Limited multi-bank acceptance — 10 vendor applications	— In-house PKI infrastructure — 20K - 100K users — File signing and web-banking — Multi-bank acceptance — 10 vendor applications

(Fig. 8) Three case studies

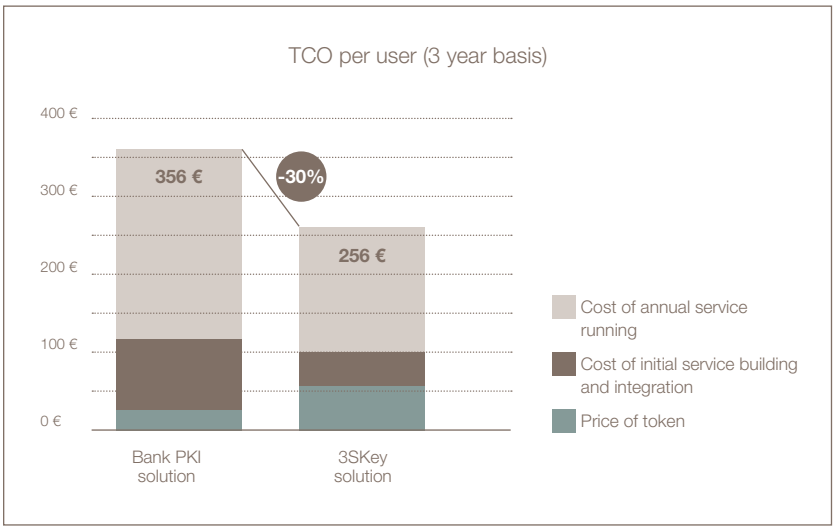
Case Study 1 – Institution small user base and limited needs

This scenario looks at an institution with a small user base ranging between 1,000 and 10,000 users that has limited needs and outsources the solution to a PKI service provider. The organisation uses digital certificates only for its application-to-application file exchanges, no web banking integration is necessary. Also, the organisation has no need for multi-acceptance of its digital certificates with other financial institutions.

The organisation has limited or no experience with PKI. The PKI is designed, built and hosted by the PKI service provider in its secured data centre and there is limited interface customisation to avoid costly development. Also, the tokens are chosen and qualified by the service provider. In this scenario, the cost of the tokens represents only 6% of the total costs (Fig. 9)

Cost component	3-year TCO per user
Annual maintenance and support	69%
Initial build and integration	25%
Token	6%

(Fig. 9) Cost break-down using a third party with 3,000 users and limited needs



(Fig. 10) 30% cost savings for institution with small user base and limited needs

The user registration is performed face-to-face at the local branches. The technical aspects for registering the users are performed by registration operators in the central back-office; with an average of one operator available for 1,000 users. The helpdesk tools are limited and the first line support for users is performed by the institution itself, whereas more complex and technical cases are escalated to the PKI service provider.

The customer base in this scenario uses on average five common financial software applications. The institution ensures optimal integration of its digital certificates with the vendors of these applications, a set of APIs are made available by the PKI service provider. Typically the effort to support integration with five vendors is estimated to be 30 man-days (3-year basis).

The institution does not subscribe to an insurance plan for its PKI. The PKI service provider is audited once a year, therefore the institution will rely on the audit controls of its PKI provider.

The result of the analysis demonstrates that with 3SKey the TCO per user over three years can be reduced by 30% compared with a third party PKI service provider (Fig. 10). This represents potential savings ranging from 200K EUR to 700K EUR depending on the number of users. On top of the cost savings, this kind of institution will also minimise its project risks, have a transparent view on the total project budget and benefit from additional services at no extra cost. Examples are multi-bank acceptance, assured 3SKey support with a growing number of financial application vendors and a possible leverage of the 3SKey digital certificates for on-line web banking services.

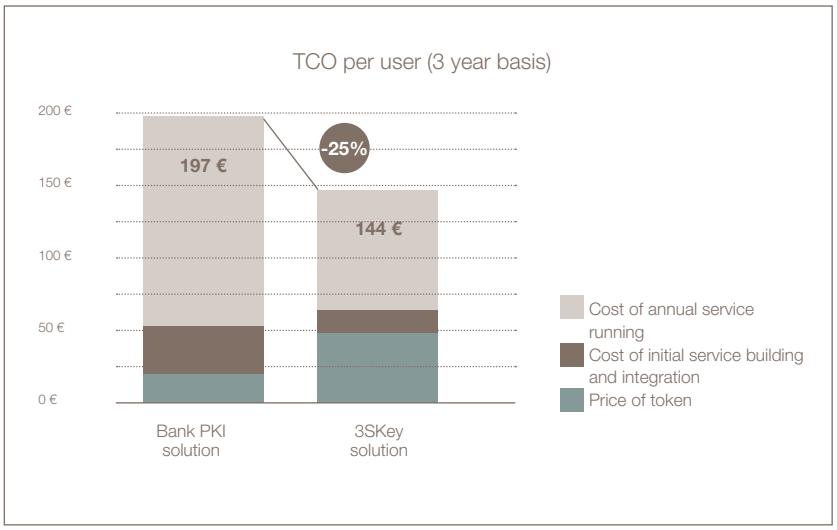
Case Study 2 – Institution with medium-sized user base and regular needs

This scenario reviews an institution with a medium-sized user base ranging between 10,000 and 50,000 users. It has regular needs and already uses a PKI solution outsourced to a PKI service provider. The organisation uses digital certificates for authentication and digital signatures on its bank web portal, as well as for its application-to-application file exchanges. The organisation requires its digital certificates to be accepted by two other financial institutions. Typically the effort for multi-bank acceptance is estimated to be 30 man-days per additional bank (3-year basis).

The institution already uses PKI and therefore has acquired experience with such technology. The PKI is designed, built and hosted by the PKI service provider in its secured data centre. In this scenario, the institution has customised the PKI interfaces to let customers manage their own company administrators and users. Also, workflows are developed to automate the issuance of new certificates and the renewal process. The tokens are chosen and qualified by the service provider. In this scenario, the cost of the tokens represents only 9% of the total costs (Fig. 11).

Cost component	3-year TCO per user
Annual maintenance and support	74%
Initial build and integration	17%
Token	9%

(Fig. 11) Cost break-down using a third party with 15,000 users and regular needs



(Fig. 12) 25% cost savings for institution with medium-sized user base and regular needs

The initial registration of the company administrator is performed face-to-face at the local branches; afterwards the company administrator registers and manages their users. The technical aspects for registering the users are performed by registration operators located at each of the 20 regional back offices of the institution. Helpdesk tools are developed to ease user deployment and limit calls to the support centre. First line support for users is performed by the institution itself, more complex and technical cases are escalated to the PKI service provider.

The customer base in this scenario uses on average 10 common financial software applications. The institution ensures optimal integration of its digital certificates with the vendors of these applications, a set of APIs are made available by the PKI service provider.

The institution does not subscribe to an insurance plan for its PKI. The PKI service provider is audited once a year, therefore the institution will rely on the audit controls of its PKI provider.

The result of the analysis demonstrates that with 3SKey, the TCO per user over three years can be reduced by 25% compared with a third party PKI service provider (Fig. 12). This represents potential savings ranging from 700K EUR to 1,800K EUR depending on the number of users. On top of the cost savings, institutions with multi-bank acceptance requirements will benefit from extended interoperability with more financial institutions as 3SKey is being further adopted in all markets. They will also take advantage of keeping the solution up-to-date as technology evolves and they do not have to manage the integration and evolution with existing and new financial application software vendors.

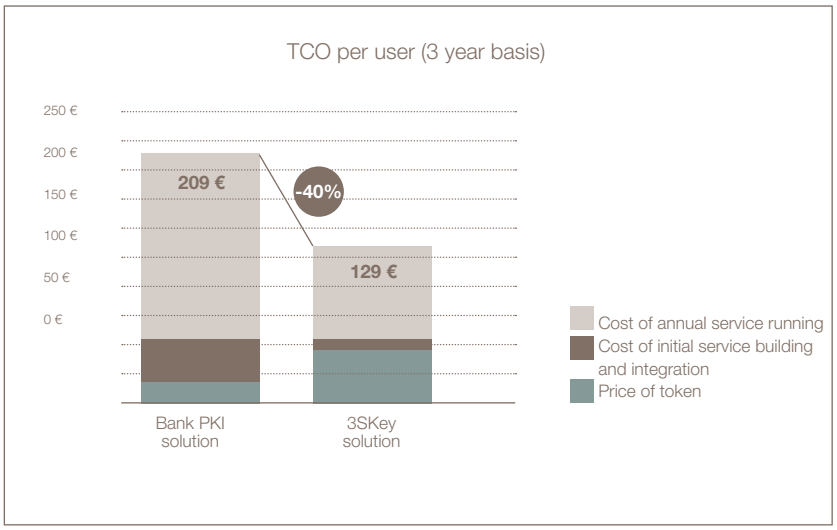
Case Study 3 – Institution with large user base and extended needs

This scenario analyses an institution with a large user base ranging between 20,000 and 100,000 users, who has extended needs and runs an in-house PKI infrastructure. The organisation uses PKI authentication and digital signatures on its web banking portal and also for its application-to-application file exchanges. The organisation requires its digital certificates to be accepted by five other financial institutions.

The institution has decided to create an in-house PKI and design and host it in its secured data centre. The organisation has already very good expertise on PKI and an experienced team in such technology. The physical data centre and logical security frameworks are not specific for this project but shared with other existing critical bank infrastructures. They buy and configure the necessary software and hardware themselves. The tokens are chosen by the institution itself and are already supported by the PKI software. In this scenario, the cost of the tokens represents only 7% of the total costs (Fig. 13).

Cost component	3-year TCO per user
Annual maintenance and support	77%
Initial build and integration	16%
Token	7%

(Fig. 13) Cost break-down using an in-house PKI with 30,000 users and extended needs



(Fig. 14) 40% cost savings for institution with large user base and extended needs

The initial registration of the company administrator is performed face-to-face at the local branches; afterwards the company administrator registers and manages their users. Five CA administrators are trained to maintain and monitor the solution and 30 registration operators manage the end-users. Helpdesk tools are developed and the existing customers' portal is adapted to support the deployment of PKI certificates with its customers. All user support is performed by the institution itself, only complex issues are submitted to the PKI software editor for resolution. Typically the customer support costs represent 30% of the annual running costs of the PKI service.

The customer base in this scenario uses on average 10 common financial software applications. The institution ensures optimal integration of its digital certificates with the vendors of these applications. A set of APIs developed by the PKI software vendor and configured for the institution's specific PKI are made available to the vendors.

In this case, the institution subscribes to an insurance plan for its PKI. The PKI platform is audited by an external auditor once a year.

The result of the analysis demonstrates that with 3SKey, the TCO per user over three years can be reduced by 40% compared with an in-house PKI infrastructure deployment (Fig. 14). This represents potential savings ranging from 2,200K EUR to 4,600K EUR depending on the number of users. As the number of users grow in such a scenario, the cost benefits of using 3SKey increases further for the financial institution. On top of the cost savings, an organisation avoids auditing its PKI infrastructure on a regular basis and limits the recurring investments linked with technology renewals as security paradigms change.

Conclusion – Outsource infrastructure, reduce costs and keep control with 3SKey

Implementing a PKI solution is indeed not only a question of 'keys' and 'tokens'. Many of the running and maintenance costs are not immediately visible when comparing different solutions. That's why a Total Cost of Ownership (TCO) review helps you to make a complete assessment of the real costs whether you are a small, medium-sized or large organisation with specific requirements.

Taking into account all cost components to build and maintain the service, 3SKey proves to be a cost-effective alternative to replace traditional and expensive PKI implementations (Fig. 15).

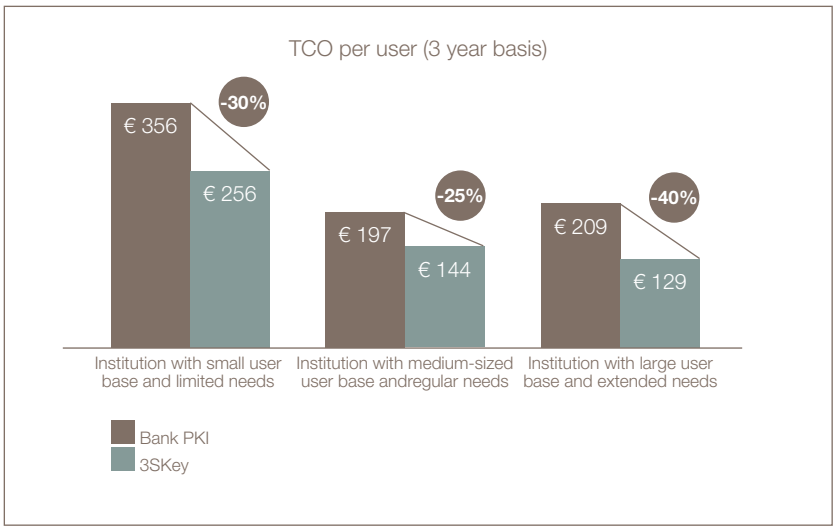
If you are an institution with less than 10,000 users and limited needs, the total cost per user could easily go down by 30% when implementing 3SKey. Additionally, 3SKey will offer a scalable solution without extra investments as the size of your institution increases, the user base grows or you plan to expand the use of digital certificates to other channels such as on-line banking services.

If you are an organisation with up to 50,000 users and regular needs, the savings with 3SKey are at least 25%. With 3SKey, you will also benefit from a solution which evolves as new technologies become available or new security threats are identified. Moreover, SWIFT works together with the industry to ensure smooth integration in the most commonly used financial software applications used by you and your customers. The use of industry standards facilitates customisation and integration with your applications.

If you are an institution with many users and tailored needs, you could even reduce your costs by 40%. As your customer base grows, so will the average cost per user be further reduced. By using 3SKey, you benefit from a proven and trusted PKI infrastructure powered by SWIFT, saving you from having to invest in and maintain your own identity management technology.

On top of the financial savings, 3SKey will provide you with additional competitive advantages, including:

- Response to a growing demand from your customers for a single solution for all their banking transactions
- Out-of-the-box multi-bank acceptance
- Retain control of the identity and KYC of your customers
- No need to rely on identity management or PKI of other institutions
- No complex contracts between financial institutions



(Fig. 15) 3SKey enables cost savings between 25% and 40% for your institution

And you? How much do you pay for your PKI solution?

Get started now with 3SKey.

If you are interested in knowing more about this cost study or you would like to tailor the analysis for your specific organisation and business needs, please contact your SWIFT representative or send us an e-mail to 3skey@swift.com.

For more information about 3SKey
visit www.3skey.com

56183 - SEP2012

3SKey

Not just another token

www.3skey.com

3SKey is a secure personal digital identity solution to reach all your banks across all channels