

Low cost trusted security – myth or reality?

A WHITE PAPER FROM WISEKEY



Contents

.....	
Analogue to digital – how have trust and security evolved?	3
.....	
Establishing a digital identity	4
.....	
Building trust between companies and individuals – where we are today?	5
.....	
Confident collaboration	7
.....	
Security and reliability	8
.....	
Legal implications of digital transactions	9
.....	
Deploying a PKI architecture	10
.....	
Removing complexity, increasing trust – the WIS@Key model	12
.....	
Trust neutrality	12
.....	
PKI for everyone	13
.....	
Opportunities for a secure future	14
.....	

Executive summary

Contrary to conventional wisdom, high-security software solutions do not need to take up your entire annual IT budget. And you don't have to discard your existing IT investments to achieve a comprehensive security solution.

Today, with technology enabling remote communication, the importance of trust – in the reliability of the data, the computers or devices used and the identity of parties communicating – is greater than ever. As a result, investing in higher levels of digital security and authentication is becoming a pressing requirement. Companies are under pressure from governments, customers, suppliers – and even competitors – to scale up the level of security they maintain in their digital transactions.

But security doesn't need to be a burden. Forward-thinking organisations treat it as an opportunity to build greater trust in their relationships. Novel approaches to what would otherwise be expensive and complex technological infrastructure projects, have been developed and are being implemented by companies such as WIS@Key. Companies that enable the deployment of high-security, enterprise-grade, flexible solutions, can now do so at a total cost of ownership far lower than had previously been thought possible.

This white paper looks at the driving need for higher security digital systems and how organisations and individuals can easily create their own trusted communities – or become part of larger trusted communities.



Analogue to digital – how have trust and security evolved?

Trust underlies the most basic transactions we conduct with people and organisations. The fundamental basis of that trust is identity – our ability to recognise the person or group of people with whom we are dealing. Without this, we cannot act with any confidence that our counterpart will perform the task or function which they promise. Before we can trust, we must first identify.

Identifying the person you want to communicate with usually involves recognising them by sight or by voice, or by having some prior knowledge of someone or something that instils trust. Even if an individual is not known personally to you, there are a number of ways of establishing a person's credentials. This can be through personal contacts, such as a friend or colleague, or through some form of independent verification such as a passport or driving licence. In the digital world, these forms of identification still exist, but they sometimes appear to us in different ways – for instance, a friend makes an introduction over the social utility web site *Facebook* rather than at the gym. Whichever form identification takes, before we can trust another party, we must first validate its identity through various layers of screening.

Once a person's or organisation's identity has been confirmed, the next stage of the process is to establish a level of trust. We will typically assess attributes of a person or organisation to gauge their trustworthiness in a given situation. Again, we can do this through personal contact, third-party recommendation, or historical reputation. We also rely on laws and regulations to determine whether the person or entity is fit for purpose and is bound by certain standards of practice or competence.

In relationships that are conducted electronically, individuals are still required to make these assessments. Just as we rely on certain assumptions when making decisions in an analogue environment, we also rely on electronic media to make similar assumptions for us. For example, is the web site we are purchasing from genuine? Will my payment reach the intended party? Will the goods purchased be delivered? These are all questions we may also ask when dealing with someone face to face.

Any person or organisation that wants to build confidence in its target audience, needs to ensure that it is trustworthy in both the digital and non-digital worlds. This is achieved through the way they conduct their relationships, which, in turn, is dictated by the policies they implement to define their activities. Many individuals and organisations will rightly define separate policies to apply to the different methods of communication or transaction. As electronic transactions become more widespread, and people become more adept at using technology – or, indeed, at trying to subvert technology – increasingly sophisticated policies and techniques of assuring identity and trust will be required.

Any person or organisation that wants to build confidence in its target audience, needs to ensure that it is trustworthy – both in the digital and non-digital worlds.

Establishing a digital identity

So how can we build trust in the digital world? Identity and access management (IAM) goes a long way to achieving this goal. IAM is the set of processes and supporting infrastructure for creating, managing and using digital identities, and enforcing security-related business policies.

The two constituent parts of IAM manage separate processes.

Identity management is a process for managing the entire lifecycle of digital identities and profiles for people, systems and services. It is the mapping of traditional processes to the Internet-connected world and typically includes:

- Automated provisioning of new users – for example, creation of ID credentials in the paper-based world
- User self-service functions – for example, changing the personal identification number on your bank card

- Workflow processes for approving account creation, modification and assignment to specific roles – for instance, change of titles, roles, jobs, schools or countries
- Removing users when they no longer require access – for instance, leaving a job or finishing a degree in a university

Access management is a process for regulating access to information assets by providing a policy-based control of:

- Who, by role, should access specific systems – for example, who can work at a hospital
- What that role is permitted to do – for example, is this person a qualified doctor?
- What permission or restrictions are on that role – for example, is this doctor authorised to work in the intensive care ward?

IAM infrastructures provide a framework for secure transactions that support both organisations' and individuals' needs for a trusted online experience.

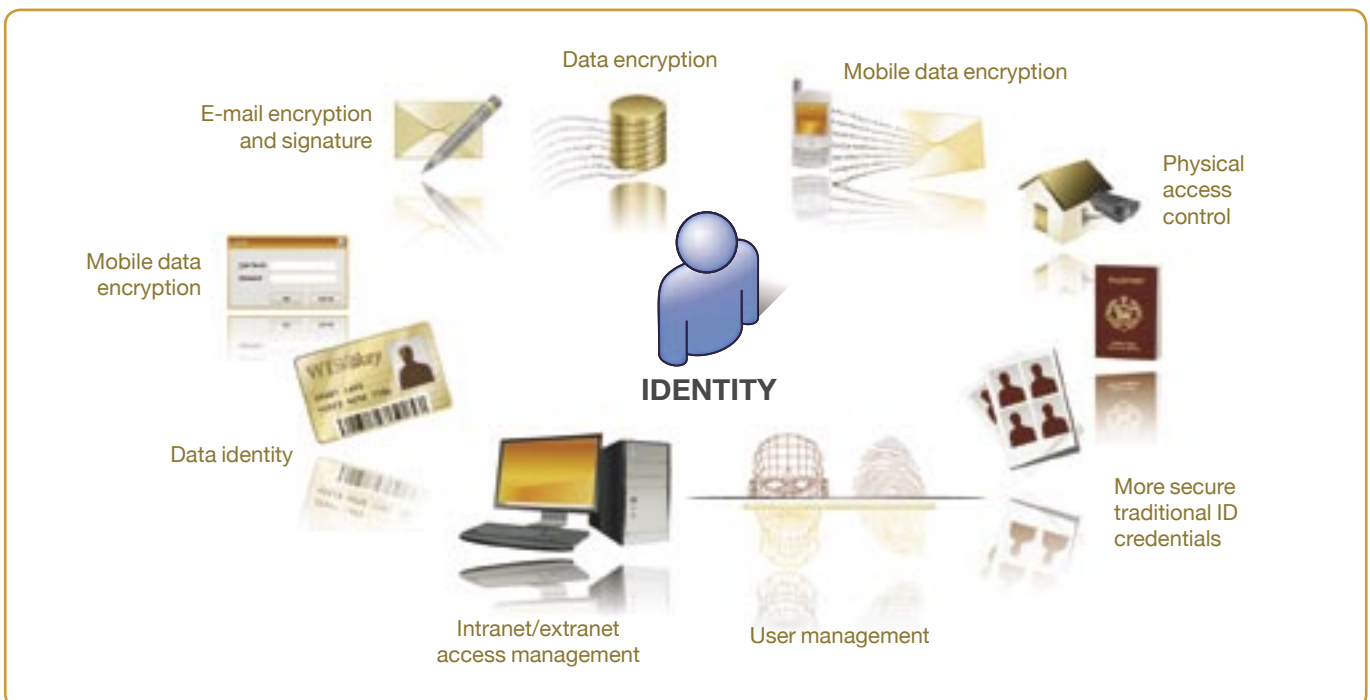


Figure 1 – Identity access management environment

Building trust between companies and individuals – where we are today

A number of factors drive the market for IAM solutions. Consumers are more concerned than ever about the security of their online information. Identity theft and the fraudulent use of instruments of payment are currently two of the top concerns. A number of recent high-profile cases have arisen – where financial institutions have carelessly disposed of paperwork revealing customer account details. Similarly, cases have been known where bulk lists of credit-card numbers have been illegally accessed and funds extracted. Understandably, this has led to widespread concern among consumers.

There are social concerns too. In more and more households, both parents now work and have less supervision over children's activities online – particularly the use of chat rooms and social networking sites. Unsupervised children can easily purchase items over the internet. Electronic games and movies may have age restrictions applied to their consumption, but because there are often no effective measures to establish the user's age, children are able to buy them.

Issues such as these should be uppermost in the minds of business executives leading organisations keen to set the pace in excellent customer relationships. In the early days of e-commerce, many companies were concerned with protecting their investment in the traditional sense of preventing 'online shoplifting'. Little thought was given initially to the corporate social responsibility aspects of their online business because pressure from consumer groups and government bodies did not have evidence of poor practices or wrongdoing. Today, astute enterprises are implementing policies that offer protection to customers against information and property theft. Brand-leading companies that have traditionally enjoyed good

reputations in their offline relationships are keen to preserve these by applying the same values to their online activities, and are quick to change policies when errors arise. By adopting this approach, these companies benefit from the continued trust of their customers. And as public pressure and governmental regulations grow, companies will need to take greater measures to ensure that the flow of personal data and property over the internet is more secure, and that transactions can be traced quickly and efficiently.

Regulatory compliance is one of the major drivers for the adoption of stronger and more sophisticated digital security measures. In certain contexts, companies' IAM technologies are beginning to be audited in much the same way as their finances are audited. Consequently, the technologies used need to include strong control and reporting functionality. The extent and severity of regulations varies from country to country. Multi-national companies are under pressure to interpret regulations for each location in which they operate and apply appropriate policies. We can see that these multi-national organisations, on the whole, tend to choose the strictest regulations in force and adopt those as worldwide company policy.

While the regulations themselves rarely specify the tools a company should deploy, they do define a set of standards, practices and requirements that constitute compliance with those regulations. For example, the Sarbanes-Oxley Act in the United States requires that chief executive officers and chief financial officers of publicly traded companies personally ratify their companies' accounts, and attest to the internal controls that guarantee the validity of those accounts. To comply with

Continued »

this, companies need to adopt strong business processes. Confidence in the controls and reports required to endorse financial and operational statements that have to be submitted means digital security is central to these processes.

Typically, a company will need to prevent unauthorised access to documents and applications, from outsiders as well as internal staff with legitimate access to the corporate network, but not to specific content. Audit trails are also needed to prove that no content has been accessed by unauthorised users, or any access rights have been violated. When content is accessed by legitimate users, the individual who accessed it, the time and date, and the nature of any changes that were made will also be tracked and stored.

According to a CIO Insight survey (see Figure 2), while IT spend on compliance is stabilising, the majority of organisations

believe that their investment in security and business continuity would be much less were it not for Sarbanes-Oxley and HIPPA regulations¹. In fact, in a more recent report, 62 per cent of respondents believed it was likely that in the next five years a chief information officer would be jailed for his or her company’s Sarbanes-Oxley violations².

As regulatory intervention in all countries increases, so the importance of software tools to assist in assuring compliance remains high. However, over time, the focus of that spend will evolve from deploying software to meet immediate needs, to the search for longer term cost efficiencies in compliance management.

¹ HIPPA – These are regulations in the United States governing the protection of individuals’ medical records and other personal health information.

² CIO Insight, January 2007

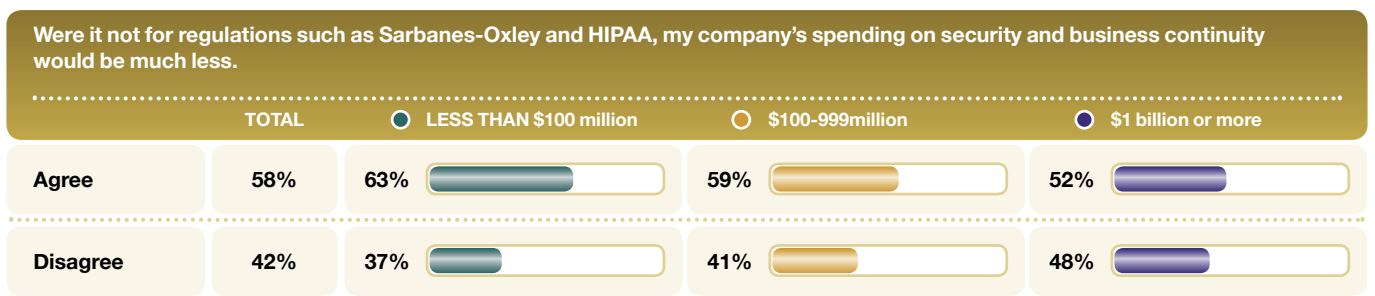


Figure 2 – Source: CIO Insight, June 2006

Confident collaboration

With new and emerging markets, enterprises are extending their reach beyond their organisational boundaries as well as traditional geographical boundaries. Being able to work effectively and flexibly without exposing itself to increased risk is an important factor to consider when looking into extending an organisation's business. Whether it's through creating an office in a new location, merging with or acquiring another enterprise to gain access to new markets, or temporarily creating teams across organisations, extending an enterprise infrastructure carries risks as well as opportunities. As the network widens, the right people need controlled access to the right resources. Protecting enterprise information is essential. But it should not be at the expense of integrity, confidentiality and diligent management of intellectual property rights.

Enterprises that are looking to provide flexible working practices and support mobile workforces typically will face many of these challenges. Previously, mobile workers would need to return to the office to place orders, file paperwork or collect new appointments. As mobile devices become more widespread, more communications and transactions are taking place away from the office, often over unsecured networks. E-mail, mobile customer relationship management and other forms of network access are helping individuals and companies to become more productive. For instance, in the United Kingdom, research shows that around 87 per cent of remote workers use their home PCs to access company data. Of these, 90 per cent admit they are responsible for maintaining security on their PCs³.

This fact alone demonstrates the clear need for strong security policies regarding access to corporate networks. Many individuals are not aware of all the dangers outside their PC and how their personal IT assets are being accessed. With wireless networking becoming ubiquitous in the home there are additional concerns – for example, the potential for pharming attacks, where wireless routers are open to firmware alterations if users do not adjust the administrator settings and access rights. Companies therefore need to balance the benefits of mobilising their employees against the costs of securing their networks from external attack and choose appropriate safeguards against malicious activities.

Businesses also need to balance these same equations when working with third parties. As competition becomes fiercer, many enterprises are looking to collaborate with partners to realise new business objectives. Information exchange is at the heart of this. Organisations need to open up their networks – or defined portions of their networks – to entities outside their corporate firewall, which exposes the organisation to new threats. People outside an organisation generally are not subject to the same company rules or policies as an employee would be. The result of this is that there are limitations in the number and type of sanctions against misuse an organisation is able to impose. Therefore, in addition to technology-based protection, non-digital policies to control behaviour on their networks should always be assessed and implemented.

³ Research carried out by TNS and Bourne Vanson for ZyXEL..

As competition becomes fiercer, many enterprises are looking to collaborate with partners to realise new business objectives.

Security and reliability

Online fraud is on the increase. Direct losses from fraudulent access to private information are often just the beginning. When other factors are considered, such as legal fees arising from litigation, regulatory fines, the costs of countering bad publicity, as well as the costs involved in closing security holes, the amounts involved can rise dramatically. Some estimates in the United States put the cost of security breaches at between \$100 and \$182 per compromised record – some estimates almost double these figures. For large-scale breaches this means companies could potentially face costs into millions of dollars.

The methods used to breach security have become more varied. Phishing attacks, for instance, are becoming increasingly sophisticated. Companies can also be exploited through their employees, leaving data and financial applications vulnerable to theft or attack. According to MessageLabs, on 12 September 2007 more than 1,100 high ranking company executives worldwide were deliberately targeted. The e-mails sent to them claimed to be from a recruitment firm and mimicked a Microsoft error message to trick recipients into clicking on a malicious attachment. Assuming these executives have legitimate access to highly sensitive company data and systems, the potential threat is clear.

The methods used to breach security have become more varied. Phishing attacks, for instance, are becoming increasingly sophisticated. Companies can also be exploited through their employees, leaving data and financial applications vulnerable to theft or attack.

Legal implications of digital transactions

In addition to compliance regulations, the legal exposure organisations are subject to do not change in the electronic world and therefore need to be conscientiously assessed. Secure identity and access management technologies play a key role in ensuring the substantial reduction of legal risks to companies.

For example, in the past, ensuring third-party compliance with obligations of confidentiality meant storing documents in a locked office and/or filing cabinet. Today, much of the same confidential information is stored electronically and is accessible remotely. Ensuring that only authorised people access such data – and that its use be in compliance with any confidentiality undertakings – depends on ensuring secure identity and access management systems. This is just one example of a wide variety of areas in which organisations are having to manage their increased legal exposure due to the popularity of their web sites. Other areas that affect organisations include:

- Protection of intellectual property rights: ensuring that the person developing any intellectual property is bound by the appropriate terms to guarantee those rights are allocated to a specific organisation. For example, the cross-organisational collaboration scenario where it is sometimes unclear who retains the IP developed.
- Ensuring compliance with data protection regulations: organisations regularly share all sorts of data concerning their employees, partners and customers that may even include sensitive data such as race or political affiliations.

IT has increased the facility with which this is done as well as the risks of infringing the data protection laws applicable across Europe and many other countries worldwide.

- Ensuring service levels with customers: ensuring the security of operations to meet contractually binding service levels is essential. The identity of individuals operating these services, as well as their access, is key to reducing the risk of not meeting the service levels and those exposing an organisation to liability.
- Dematerialisation: the digitalisation of documents – for example, invoices and accounting records – is widespread but compliance with the applicable law is becoming an increasing problem for organisations. Non-compliance with such regulations can result in hefty fines and, in some cases, criminal proceedings.

Other legal exposure areas are more specific to certain industries such as the financial services sector, health sector and defence contracting.

The points outlined above represent some of the challenges faced by individuals and organisations. As techniques evolve to take advantage of security weaknesses, so do the laws, practices and technologies designed to counter them. In the past, the ability to implement policies and technologies that can enable high-security protection of physical and information assets have been mostly the preserve of large organisations. Today there are technologically advanced solutions available that are simple to deploy and do not require investments of millions of dollars. WISeKey is at the forefront of developing and deploying these technologies.

Deploying a PKI architecture

Historically, systems providing the highest level of security have been those based on public key infrastructures (PKIs). A PKI is an arrangement that binds public cryptographic keys with respective user identities by means of a certificate authority (CA). The user identity must be unique for each CA. Identity validation is carried out by software at a CA, usually based on some form of human supervision, together with other coordinated software at distributed locations. For each user, the user identity, the public key, their binding, validity conditions and other attributes are not susceptible to forgery in public key certificates issued by the CA. The infrastructure typically is also composed of: a lightweight directory access protocol (LDAP) directory; a CA; a Registration Authority (RA); Certificate Revocation Lists (CRL) that can get unwieldy when they are checked; Online Certificate Status Protocol (OCSP), screening certificates in real time; and digital certificates that must be issued to all parties before they can use the PKI.

When deploying PKI, much importance has been placed on training all users how to keep their certificates secure – even when they upgrade their computers, or have them repaired.

Putting this into practice in a large organisation has proved far more expensive to deploy than was initially imagined. The reason for this has been due typically to simple under budgeting, complex business process audits and subsequent re-engineering, along with the cost of setting up CAs and other related systems. Other causes for complaints are that the operational costs of maintaining the infrastructure, keys, hardware and specialised data centre operations.

These so called horror stories certainly have their basis in truth. It is also true that many security software vendors sell full-scale, in-house PKI solutions that do have large up-front costs, as well as high ongoing support and management overheads.

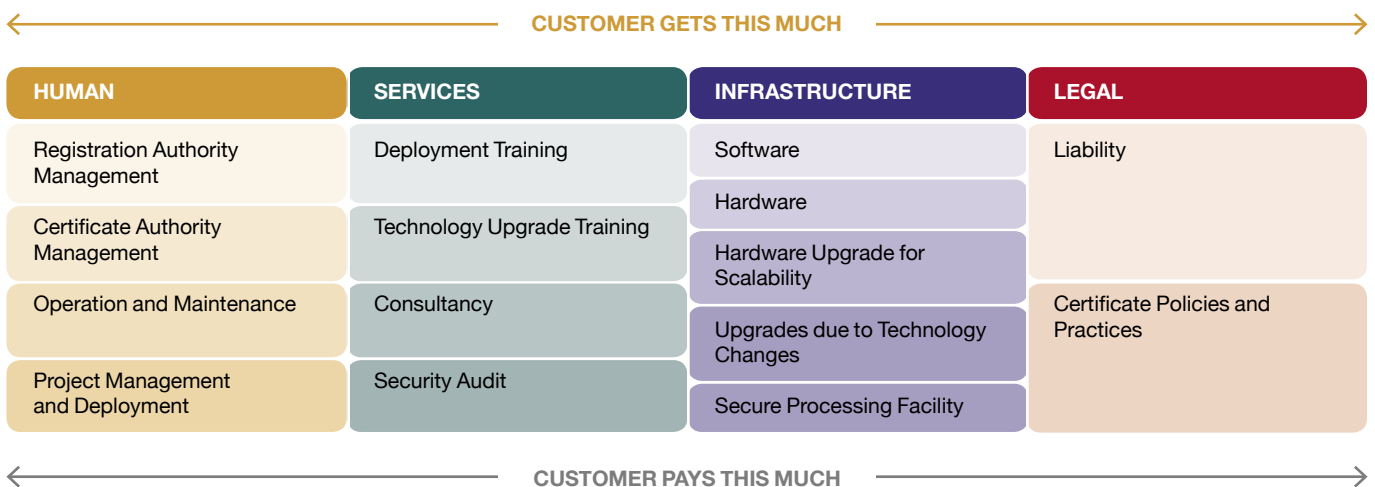


Figure 3 – Typical in-house PKI implementation

Some large organisations can afford to make these investments and will do so if they believe the benefits will justify those costs. Other organisations may not be able to justify the investment, but require the same high level of security. Previously these organisations have had to make do with systems that offer lower levels of security or trust.

As an alternative to this in-house model, certain companies offer a managed model by which the infrastructure is located centrally in a shared environment. This enables organisations to relatively (but not substantially) reduce the costs and complexity of implementing PKI. This approach, however, has had several problems over the years, including:

- The centralised location of sensitive data – bank customer identities
- Loose integration with the backend systems of organisations – making seamless identity and access management difficult
- Full dependence on an external organisation for security of sensitive activities
- Geopolitical concerns – many of the managed service providers operate out of the United States

Some debate has taken place as to whether alternatives such as Pretty Good Privacy (PGP) are better than PKI. PGP and other alternatives have their benefits – a lower cost of deployment may sometimes be quoted as one of them. However, their drawbacks, such as requiring client software at the sender and recipient ends or not having the scalability of PKI, tend to outweigh the benefits.

Certificates are the commonly accepted method for authenticating and protecting valuable transactions, beginning with their fairly transparent use in enabling secure socket layer (SSL) web sites.

Certificates are also supported in all major web browsers, which is not the case for PGP keys and other alternatives, allowing easy client authentication.

So much so, that the majority of enterprises are now preferring PKI over alternative solutions. Today, vendors such as WISEKey offer highly secure PKI solutions that are cost efficient to both deploy and maintain.

PKI solutions also bring benefits such as much broader operating system and application adoption. Certificates are the commonly accepted method for authenticating and protecting valuable transactions, beginning with their fairly transparent use in enabling secure socket layer (SSL) web sites. Certificates are also supported in all major web browsers, which is not the case for PGP keys and other alternatives, allowing easy client authentication. The same is true for secure devices such as smart cards and USB tokens.

Removing complexity, increasing trust – the WISEKey model

WISEKey has been analysing the issues surrounding security for many years. The company’s specialists have experience of highly sensitive environments – for example, they were involved in first ever legally binding Internet voting system – as well as highly complex environments with technologically challenged infrastructures, such as in developing countries. WISEKey has built on the lessons learned and made the security, reliability, cost effectiveness and practicality of using PKIs a reality. As a result, WISEKey has put sophisticated PKI implementations within reach of organisations of any size, as well as individuals.

The WISEKey model is unique in two ways:

- 1) It offers a totally neutral trust model founded on its Swiss origins and its association with the Organisation Internationale pour la Sécurité des Transactions Electroniques (OISTE) foundation
- 2) It brings PKI benefits to the mass market at an affordable price by taking advantage of the PKI technology built-in to Microsoft Windows Server software

Trust neutrality

With its headquarters in Switzerland, WISEKey operates under Switzerland’s established political neutrality, security, confidentiality and efficiency laws. These are all essential requirements for the mass deployment of secure identity and access management infrastructures.

WISEKey acts as the business operator for OISTE root cryptographic keys. The OISTE Foundation is a non-profit international organisation based in Geneva, Switzerland. Founded in 1998, OISTE was created with the objectives of promoting the use and adoption of international standards to secure electronic transactions, expand the use of digital certification and ensure the interoperability of certification authorities’ e-transaction systems.

The OISTE/WISEKey root is an offline root certificate for signing certification authorities and backed by OISTE. It is the basis for all other certificates issued through not just WISEKey solutions, but any other solutions accepted by the foundation, which are able to comply with the policies and practices that are applicable (see Figure 4). The OISTE/WISEKey root systems were created and maintained in a secure bunker under the Swiss Alps recognised as one of the most secure areas in the world today. Because of Swiss confidentiality

laws, no private or government body can force the root key to be divulged. This guarantees that all information and data en-crypted through OISTE/WISEKey certificates will remain secure. This approach is unique as no other infrastructure of its kind exists in such a high security environment, and the level of neutrality and protection afforded by stringent Swiss confidentiality and security laws is second to none.



Figure 4 – The OISTE trust model

PKI for everyone

WISeKey recognised some of the challenges faced by large and small organisations in deploying PKIs. WISeKey has been involved in large scale PKI projects with some of the world's largest private and public sector organisations. As the company developed its expertise in managing these deployments, it was also quick to recognise where problems arose, and where costs could be controlled.

As a result, WISeKey has developed a suite of products that reduces complexity and costs at a stroke by enabling its products to benefit from the digital certification technology already built in to the Windows Server platform. This suite also provides specialised, high-security components that extend and enhance the Microsoft technology into a full-scale industry strength PKI.

This approach means businesses of any size are able to develop enterprise class security policies in the knowledge that they can make full use of their existing technology investments to help put the policies into practice.

This approach also allows WISeKey to provide companies with the flexibility and scalability they need to satisfy their own requirements. Companies can choose to deploy a framework hosted entirely within their own facility, or partner with WISeKey to implement a managed service hosted at WISeKey's secure data centre. In essence, the approach taken by WISeKey can provide certification services to a two to five person company all the way up to a national identity system, with very flexible forms of deployment, be it in-house, managed, ASP mode or a series of other hybrid combinations of these.

Individuals can benefit too. Employees within an organisation can use the trusted electronic Identity (eID) not just in their business activities, but their personal lives too. If an individual wishes to create a personal eID, they can do so by using their company CA to validate their ID with WISeKey directly and obtain an ID that is not linked to the company for which they work. This provides a trusted eID, which they can use wherever they are, and on any secure storage device that will be accepted across the internet for secure communications and transactions.

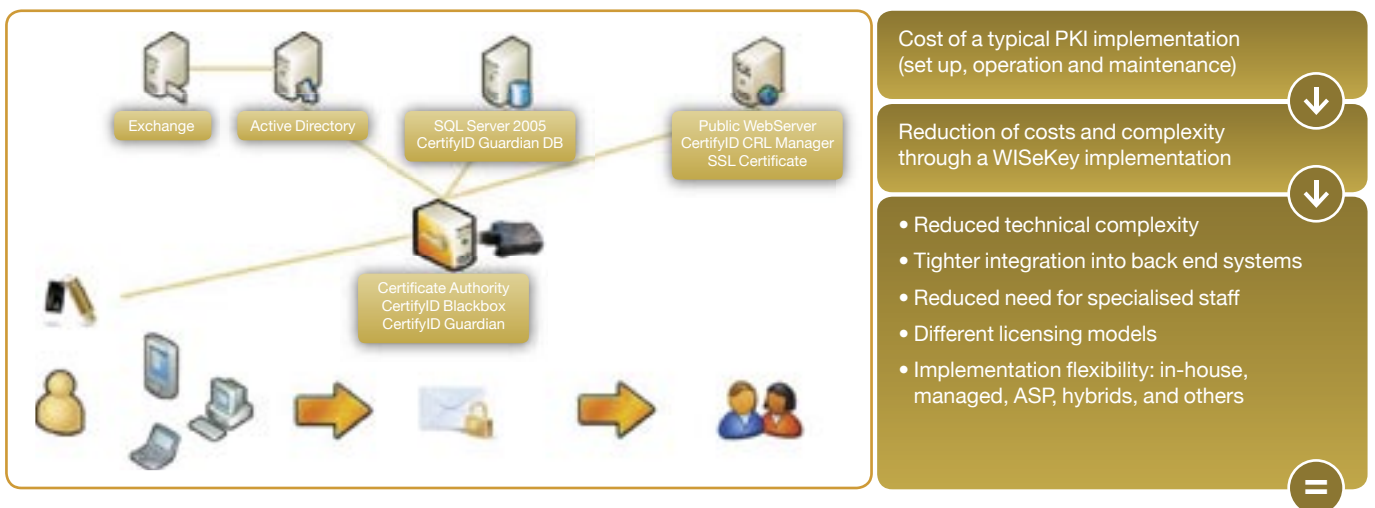


Figure 5 – WISeKey PKI implementation

Opportunities for a secure future

More people than ever are using the internet to make purchases, manage finances and complete tax returns – to name but a few transactions. It is also true to say most consumers are suspicious of internet security. However, all the signs show that despite the suspicion, people's confidence in using the internet for these sorts of transactions is growing. This evolution is also affecting businesses. Mobile devices and the infrastructure required to support them is making a compelling business case for enterprises to change the way they do business and companies of all sizes are quick to see the competitive benefits in mobilising their operations.

Statutory requirements are difficult to predict because laws change to reflect current social and economic realities. As government regulations catch up with technology and requirements for compliance and reporting increase, the need to manage these processes over digital networks will increase. Organisations that are able to monitor and authenticate their transactions efficiently, and ensure that the privacy of the data they hold is maintained will be better positioned to adjust to future requirements of this nature.

Similarly, it is difficult to predict who you will be doing business with tomorrow, next month or next year. Your competitor today may become your trading partner tomorrow. Being able to collaborate and exchange information according to the requirements of a partnership could be crucial to success. Securing information access portals that facilitate this type of activity without risking exposure of company secrets to unauthorised parties will become ever more important. It could even make the difference between winning and losing a lucrative trading partnership.

Customers are becoming more sophisticated in their use of online resources, and are sensitive about the privacy and security of their data. When enterprises fail to take this seriously and breaches occur, the speed at which these lapses are communicated to others can be breathtaking. This can create significant problems in retaining the trust of existing customers and attracting new ones. Companies that look to harness security technologies with the aim of enhancing customer confidence, the relationship of trust, and ease of use they experience when managing transactions online, will gain a significant advantage over their competitors.

Successful companies are looking to IAM as a central force in their strategy to manage these risks and realise the opportunities that increased security investments can produce. After many years of waiting, using PKI-based IAM as a basis for secure communications is now becoming a viable solution for organisations of all sizes, not just large corporations or government agencies. Enterprises should be looking at security and privacy as a business opportunity to future-proof their regulatory compliance requirements, streamline their business operations and increase customer trust. Companies that regard it as a necessary evil – one that must be endured in order to minimise their own legal or commercial liabilities – may find themselves outperformed by more visionary competitors.

Enterprises should be looking at security and privacy as a business opportunity to future-proof their regulatory compliance requirements, streamline their business operations and increase customer trust. Companies that regard it as a necessary evil – one that must be endured in order to minimise their own legal or commercial liabilities – may find themselves outperformed by more visionary competitors.



WIS@key

The World Internet Security Company

For more information on WIS@Key
solutions please contact:

info@wisekey.com

Or visit:

www.wisekey.com

WIS@Key

WTC II

route de Pré-Bois 29

P.O. Box 885

CH-1215 Geneva 15

Switzerland

Telephone: +41 22 594 3000

