



KEYNECTIS

PRESS KIT



Protecting your **identity**
Protecting your **freedom**
in a connected world





Summary

1. Identity	3
2. About trust	4
3. Spectrum of users needs	6
4. Added value and referencing	10
5. References	12
6. Glossary	14



1. Identity

Name: KEYNECTIS

Created: July 2004

Business:

- Protect your identity,
- Protect your data,
- Protect information exchanged in a connected world.

Mission:

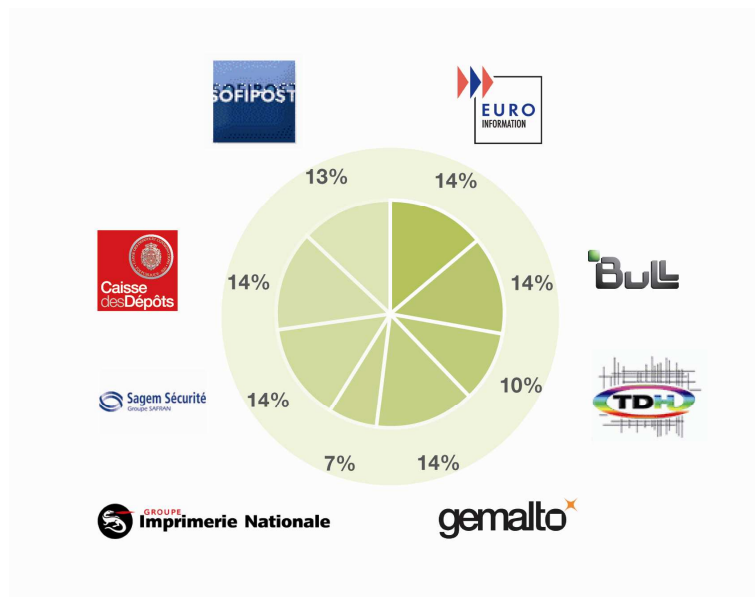
- Facilitate recognition and Trust among people.
- Give individuals the Power and Freedom to affirm their identity in everything they do,
- At all times, wherever they are.

Contact:

11-13, rue René Jacques – 92131 Issy les Moulineaux Cedex - France
Phone: +33 (0)1 55 64 22 00 - www.keynectis.com

Shareholders:

Keynectis benefits from a strong shareholder base comprise of leaders in a range of sectors. M. Thierry DASSAULT is the Chairman of the Board.





2. About trust

The tremendous development of technologies mushrooming around the Internet exposes your firm's computers to the outside world, making its network easy to penetrate and critically increasing the risk of piracy, destruction, and spying.

You must now address the following technological challenge: converting your digital work space into an area of trust.

In this perspective, the role of an area of trust consists in concentrating the security services required by the firm's projects. The stake is not only to "secure" the network; it is now also a matter of «signing», «authorizing», of «certifying».

Among your major concerns linked to Internet security are the following:

- Authentication: ascertain the identity of the party with which you are communicating
- Confidentiality: encrypt the data you are transmitting
- Authorization: ascertain the other party is authorized and vice-versa
- Integrity: be assured that the transmitted data is not altered
- Non repudiation: have the proof that the other party has indeed received your message and vice-versa

For these functions to be ensured, a certain number of resources must be installed, which are collectively known as the concept of Trust Infrastructure or Public Key Infrastructure (PKI).

The notion of public-key (also, more generally, called asymmetric key) cryptography in which two different but mathematically related keys are used: a public key and a private key. A public key system is constructed so that calculation of the private key is computationally infeasible from knowledge of the public key, even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair. In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. The public key is typically used for encryption, while the private or secret key is used for decryption.

At the core of the technologies involved: the electronic certificate, also called digital certificate. A virtual electronic passport, inherent in the notions of electronic signature and encryption, the electronic certificate enables the parties to an electronic transaction to be authenticated.

In broad terms:

- In paper world, 2 persons trust themselves (and prove their identity) when producing their identity card or passport
- In Internet world, 2 persons trust themselves using an electronic certificate



The electronic certificate is the technological cornerstone of most secured electronic interchanges.

- To guarantee the identity of individuals: electronic certificates, which can be associated to biometrics, allow, within the framework of national identity programs (passport, ID card, and health card), identity fraud and migratory flows to be controlled, this by rendering these documents tamper-proof and unique for each individual.
- To modernize the Institution <-> user relationship: by providing reciprocal online authentication, confidentiality of interchanges, and electronic signatures, the certificate enables the Institution <-> user relationship to be reversed: it is the counter which comes to the user via the Internet, and not the user who has to go to the counter. In addition to the users' relief, the result is also an increased productivity of the administrative services/users transactions.
- To protect local industries by enabling them to secure their data: while being aware of the need to protect their sensitive data, businesses are not familiar with the risks of industrial or commercial espionage. Therefore they need to be able to consult a local, specialized, trust player who can offer simple and effective securization solutions.



3. Spectrum of users needs

Signature

I sign with K.Sign® and K.Websign®

We all communicate more and more, with increasing speed. We share a growing amount of information and creative work: professional, confidential, contractual, official and personal.

As communication technology saves us time while boosting our competitive edge and productivity, it has become indispensable. But how can we sign our communication, creative work and transactions in the digital world as easily as in the physical world? How can we give digital communication the legal value that we need?

KEYNECTIS proposes services aimed at eliminating the use of paper for your business processes, documents, contracts, purchase orders and invoices. It is available online in ASP mode (Application Service Provider).

Moreover, KEYNECTIS proposes a solution which enables document usage continuity, thus reducing the need for paper documents. Thanks to this solution, KEYNECTIS can inscribe digital signatures on PDF documents while guaranteeing the ease of use as a signed paper document.

- With K.Sign® you sign documents on your computer using a personal (cryptographic) USB key, directly implemented via the desktop tools menu (Adobe® Acrobat®, Microsoft® Office, Open Office, etc.).
- With K.Websign® Web users sign documents online via a secure channel. There are no system prerequisites to perform this operation, which functions with all currently available Web browsers.



Identity

I travel with Sequoia[®] e-passport

Increasing threats and identity theft have driven the international community to reinforce border control security, and therefore travel document reliability.

Efforts made by the ICAO (International Civil Aviation Organization), in charge of setting standards for travel documents and the associated production and verification practices, have led to the definition of specifications used by industry players to implement electronic passport systems.

- **Electronic Passport:** Passport data (name, date of birth, picture, etc.) is digitally signed by the National Authority using strong cryptography and is stored on the contactless chip in the passport. This government controlled production process makes the electronic passport a legitimate and unforgeable document. During verification, the stored data is compared with the optically read data. This procedure is commonly known as Basic Access Control (BAC).
- **Biometric Passport:** E-Passport infrastructure is designed to secure biometric data (fingerprints or iris) stored in the e-passport chip and prevent cloning of the document. A reader (IS, Inspection System) is authenticated by the e Passport using cryptography. By means of this technology, the issuing country can decide which countries are granted access to the biometric data stored in the citizen's passport. This scheme is commonly known as Extended Access Control (EAC).

Electronic and biometric passports secured by Keynectis provide the best possible protection to Governments, enforcement services, customs authorities as well as users, thanks to the Sequoia[®] e Passport technology.



Authentication

I prove my identity with K.Access®

In a world where we are every day more connected via more channels, more often, it is even more important to be able to be recognized, and to prove our identity to others in order to communicate, dialogue and make secure transactions. How to get freedom, simplicity and security in one solution?

Most authentication methods require dedicated equipment that needs to be connected and transported. K.Access® enables the user to be strongly authenticated by using any standard USB storage key or other mass storage media (iPod, mobile telephone, etc.).

K.Access® is first loaded on the key by using a secret initialization code provided by the bank. Financial organizations can choose any secure method for distributing the initialization codes (SMS, email, PIN mailer, face to face, etc.).

Once loaded, K.Access® is immediately available and automatically protected by PIN code. No data is lost on the key and it can continue to be used for storing files, photos or MP3 files as usual. Users can benefit from complete mobility and connect their USB key to any computer.

Nothing is left on the computer after K.Access® is disconnected.



Validation, proof

I certify with Certify.Center[®]

At a time when electronic exchanges, communications and transactions are becoming economically strategic, it is critical to develop certification solutions that secure not just data but people too.

But how can we certify, hassle-free, the thousands of documents produced daily by our organization? How can we formalize important documents to ensure that they are heard and seen amongst millions of electronic messages?

Certify.Center[®] is a smart, powerful and ultra-secure application that automatically manages the certification process for all data and documents sent, received and archived.

With Certify.Center[®], each step of the certification process guarantees the security of the content and promotes collective trust: signature and validation are automated; security-enhancing measures are simplified.

- Certify.Center[®] signature formats: XADES, XML DSIG, PDF.
- Time stamping: RFC 3161
- OCSP validation: RFC 2560, CRLv2, http, LDAP
- Digital certificates: X509v3, CRLv2

Certify.Center[®] is delivered either under service mode, software mode or server.



4. Added value and referencing

KEYNECTIS operates a bunker-type data center that meets the most stringent **requirements in terms of physical and logical security** and produces digital certificates for our customers.

In time, KEYNECTIS has acquired in France an unrivalled expertise in those new domains of digital certification and this thanks to the following contributing factors:

- Sharing experience with other European and North-American operators and making use of identical technological common cores, thus enabling the technical architectures of production centers to be designed and optimized in order to better their performance level and to control increasing customer requirements,
- Being continuously confronted with the needs of major French firms and administrations, whose requirements are particularly sharp in terms of quality of service and of response time,
- Systematically participating in the market's structuring and reinforcement efforts, either through standardization actions, by contributing to the promulgation of adapted regulations, or by conducting innovative projects benefiting the whole community.

The + of the center

- A highly secured site including biometric and smart card access control, intrusion detection and video surveillance
- A redundant and security-supplied exploitation infrastructure
- Individual monitoring of sensitive components (cryptographic keys, computers, etc.)
- Security clearance and qualification of our personnel, 100% dedicated to the operation of Public Key Infrastructures
- State-of-the-art security meeting regulatory requirements



Based on standards recognized by French controls and several other governments in Europe and throughout the world, KEYNECTIS technologies provide guaranteed levels of service **that are certified by the strictest authorities:**

- CSP certified in accordance with ETSI TS 101-456 standard (Electronic signatures and infrastructure)
- Common Criteria EAL 4+ certification
- Qualified electronic signature (Directive 1999/93/EC)
- Certipath certification
- Adobe® CDS Partner certification
- CA Browser Forum certification (compatible with browsers and virtual machines >99%)



5. References

KEYNECTIS propose a range of solutions for a world of needs¹

Banks & Insurance

Secure interbank payment flows, remote retail banking, online opening of saving accounts, consumer loan, home and auto insurance, cash management, e-banking, online purchases ...

- AIG
- Allianz
- Amaguiz
- Amaline
- Attijawirafa Bank
- Axa Banque
- Banque Accord
- Banque de France
- Banque des Etats de l’Afrique Centrale
- BNP Paribas
- Boursorama Banque
- Cetelem
- Click & Trust
- CNP Assurances
- Coface
- Cofidis
- Cofinoga
- Crédit Agricole
- Euro Information
- Finaref
- GMF
- Groupama
- HSBC
- Informatique Banques Populaires
- La Banque Postale
- Le Crédit Lyonnais
- Médéric Malakoff
- Monabanq
- Mutualité Française
- Natixis
- Santiane – Groupe Zenith
- Société Générale Corporate Finance
- Sofinco
- Swiss Life
- ...

¹ List non exclusive



Industry & Services

Electronic invoicing, electronic signature, secure collaborative work, identity and flow traceability, paperless procurement processes, electronic ID management, secure email, e-commerce, ...

- Airbus
- Air France
- Areva
- Cardinal Systems
- Carrefour
- EADS
- Eurocopter
- Gemalto
- Informatique CDC
- La Française des Jeux
- Lagardère
- Pixid
- Place Internationale
- Réseau de Transport de l'Electricité
- Sagem Sécurité
- Safran
- Servier
- Thalès
- Valéo
- ...

Public sector

Electronic administration, remote procedures, e-passports, health cards, civil servant cards, online tax returns, paperless competitive tendering, vehicle licensing,

- Albanian Ministry of Interior
- Algerian Ministry of Interior
- Belgian Ministry of Interior
- ChamberSign
- E-Bourgogne
- French Armament Office (DGA)
- French Ministry of Defence
- French Ministry of Economy
- French Ministry of Justice
- French Ministry of the Interior
- French National Agency for Secure Documents (ANTS)
- French National Audit Office (CNCC)
- French National Print Office (IN)
- French National Tax Office (DGI)
- French Notary Office
- French Secretary General of National Defence (SGDN)
- French State Council (Conseil d'Etat)
- Guatemalan State Population Register
- Moroccan Ministry of Interior
- Paris Regional Transport (RATP)
- Professional Healthcare SmartCard Group (ASIP santé)
- Qatari Ministry of the Interior
- Water Board Rhin-Meuse
- ...



6. Glossary

This press kit contains acronyms and abbreviations. For a better understanding, you'll find hereto the ones usually used:

Certification Authority (CA)

A Certification Authority is a trusted third party that issues digital certificates and validates the identity of the holder of a digital certificate.

Certificate Policy (CP)

A description of the rules governing the use of a public key certificate in a particular environment.

Cryptography

Transforming clear, meaningful information into an enciphered, unintelligible form using an algorithm and a key.

Decryption

The act of restoring an encrypted file to its original state through the use of a key.

Digital Certificate

A digital certificate is a secure digital identity that certifies the identity of the holder. Issued by a Certification Authority, it typically contains a user's name, public key, and related information. A digital certificate is tamper-proof and cannot be forged, and is signed by the private key of the Certification Authority which issued it.

Encryption

The act of disguising information through the use of a key so that it cannot be understood by an unauthorized person.

Key

When used in the context of cryptography, a series of random numbers used by a cryptographic algorithm to transform plaintext data into encrypted data, and vice versa.

Key Pair

A pair of digital keys - one public and one private - used for encrypting and signing digital information.

Private Key

A cryptographic key known only to the user, employed in public key cryptography in decrypting or signing information. One half of a key pair.

Public Key

The other half of a key pair, a public key is held in a digital certificate. Public keys are usually published in a directory. Any public key can encrypt information; however, data encrypted with a specific public key can only be decrypted by the corresponding private key, which the key owner keeps secret. A public key can also be used to verify the authenticity of a digital signature.



Public Key Infrastructure (PKI)

A set of policies, processes, and technologies used to verify, enroll and certify users of a security application. A PKI uses public key cryptography and key certification practices to secure communications.

Qualified certificate

High level personal/professional digital identity assurance supporting legally valid digital signatures.

Registration Authority (RA)

A person or organization responsible for the identification and authentication of an applicant for a digital certificate. An RA does not issue or sign certificates.

Smart Card

A device that is often the same size as a credit card but that is “smart” enough to hold its own data and applications and do its own processing. Smart cards can be used to store personal information, hold digital cash or prove identity.

Time stamp

A timestamp is the digital proof that objectively enables to detect the creation time of certain data. To get a timestamp, the party that is interested in proving the creation time of the data, sends a cryptographic code to the time stamping service provider (TSP). Finding two data collections with a similar cryptographic code needs tremendous computing power, unavailable to any modern computer or computer network. The service provider returns a digitally signed proof that proves the existence of the said data collection. Since the time stamping authority sees only a cryptographic code, the confidentiality of the data is retained.



Press contact :

KEYNECTIS

Caroline DROBINSKI

Phone : + 33 (0)1 55 64 22 85

caroline.drobinski@keynectis.com

www.keynectis.com



*It's up to you to write the rest of the story.
Like all your ideas, we'll do everything we can to protect them.*



© KEYNECTIS All rights reserved.