

Certificates services benefits for the end user

Disclaimer: this white paper has been written to focus on the benefits of the usage of certificates and is addressed to end users that are most of the time not "PKI experts" or "IT security experts". For this purpose some shortcut explanations have been used in order to explain the "possible" benefits of certificates usage with the most "user friendly" IT implementation of certificates, which today is still the one and only way to broadcast security granted by the use of PKI certificates.

The fundamentals: Saying that "a certificate is comparable with an international passport and credit card" is completely correct. A digital certificate is a means of personal identity verification for cyber space.



Digital certificates are issued & maintained using a **Public Key Infrastructure (PKI)** which **guarantees a resource identity** (persons, applications and hardware devices) and is used to secure communications **between the subject of a certificate and the resource** that will use the certificate.

What does it look like? To you, probably nothing!

However, once installed either on a Smart Card or directly deployed on a device (PC, Laptop,...) it is **as if you were wearing your identity badge around your neck:**



Each time a **secured application** needs to **verify your identity**, depending on your badge holder (e.g. Internet browser), you have to **present your badge** (as shown: you select your certificate).



So what is the added value for you? In a few words, we can say that the **use of a digital certificate** will **allow** you to make the **transition from paper-based to completely electronic business processes** and also makes the **transition from physical control (passport, ID card) to digital integration via certificate**. These two transitions provide enormous **time saving** and **labour benefits** by allowing you to **use electronic companies' services securely without any non-security-friendly constraints**.

The main "**visible**" benefits for you will certainly be linked to **password management, taking away** the need for you to **care about it. The certificate does it for you!** So, the added value:

- ⇒ Only **1 certificate authentication** for all X.509 certificate standards compliant **applications**;
- ⇒ **No passwords to remember, update, or try to "fit"** with complex password policy, several times...
- ⇒ **About 50% less help desk calls** ("hello, I lost my password", "it's expired", "it does not work anymore", "I did not update it in time", and **all that type of hassle: eliminated**).

Certificates also reduce paper signature processes, as you can sign electronically, and also request a read receipt proof... with certificates!

What kinds of services will use your certificate? The answer is: **All kinds and every kind!**

The widely deployed usage of certificates can be regrouped in 5 main "trust categories": trusted messaging, trusted access, trusted private network, trusted online account activation and trusted forms.

Certificates will prove that "you are at the command", everywhere you pass: Applications automatically **rely on the identity proof** provided by your certificate and propose **personalized services**, using "Single Sign On":

- ⇒ Network authentication (certificate for VPN access),
- ⇒ Windows logon (certificate in smartcard for logon),
- ⇒ Laptop boot protection (certificate in TPM chip, in smartcard),
- ⇒ Electronic mail confidentiality, identity proof (certificate in outlook, thunderbird, lotus notes...),
- ⇒ Printed paper delivered in confidence (certificate in smartcard or on physical badge),
- ⇒ Certificate and badge site-access merging ("all in one" electronic services and physical services).

A **Single Sign On infrastructure based on certificates** will also **allow heterogeneous systems to propagate your identity over their applications**, domains, companies, and nations! X.509 certificate standards are **recognized & trusted** in worldwide shared electronic platforms such as Aerospace & Defence BoostAeroSpace (EU) or Exostar (US) **Internet collaboration platforms** → a good example of "**transition from physical separation to Internet integration**".

So why are we not using it today? Actually, we are, its technology is simply hidden by those who implemented it. And you may not know that you already use a kind of electronic certificate service every day and you have **similar usage in most of all bank debit card since 1989!** You present your **bank "certificate" to get banknotes back from an ATM...** or to validate new credits to your mobile phone operator company (also member of this "trust circle")... You also have some government initiatives, for e.g. since 2009 French civilians can pay their tax online using Government-provided electronic certificates!

So ok, saying you decide to use it, what's next?

Just use systems that use certificates... and when you **withdraw some "timesaving banknotes"** you will in reality also **save valuable time...**

↳ **and your business works only by the good use of time...**



¹ Not considering here the protection of the certificate associated key that should be done with pin protected smart card rather than Windows user logon password, requesting a definitive pin password to memorize.