The new standard for user authentication
In a world of change where business and security rules are constantly evolving, individuals, companies and institutions need better tools for managing identities and access to services. By developing a convenient, secure standard for strong authentication, Natural Security meets this requirement.

Through the combination of something I have (a personal device such as a keyfob, a mobile phone or a smart card) and something I am (my biometric data), Natural Security enables end users to be reliably authenticated and controlled to execute transactions.

Natural Security aspires to be synonymous with speed and security for secure transactions such as payment while at the same time guaranteeing both the protection and privacy of personal data.

The standard defined and maintained by Natural Security:
- Solves strong authentication challenges for physical and logical access, payment, electronic signature and access to services;
- Is universal and can be used in different contexts (online, in stores, in banks, at ATMs and vending machines);
- Meets the business needs of issuers, retailers and service providers.
How does it work?

Natural Security has developed the authentication solution of the future by combining a personal device, mid-range contactless technology and biometrics.

- The personal device, which is built around a secure element, stores both applications and data used to authenticate the user, resolving many issues related to security and privacy.
- Mid-range contactless technology provides a unique and convenient experience for users by sparing them the need to physically handle their device.
- Biometric technology means convenience and simplicity for end users (no PIN code to enter) while guarantying that the end-user is present during the transaction.

To be authenticated, customers simply place a finger on a device. It is the same user experience, gesture and device in all situations, whether for face to face or online transactions.
Benefits of convenient authentication for end users

Natural Security means convenience and simplicity for end users (e.g. no smart card to manipulate, no PIN code to enter).

The solution is universal and targets payment transactions and access to services in different environments (at home or work, over the Internet or in-store).

**Fast**
Authentication is fast as no code is required.
The customer authenticates himself by simply placing his finger on a payment terminal, an ATM or a reader connected to a computer.
The customer does not have to search and take out a card or any other means of payment from his pocket.

**Secure**
Natural Security has introduced an authentication solution that can be systematically used for all transactions.
Based on biometrics, it ensures transactions can only be completed when both the user and the device are present. The customer no longer needs to enter his PIN code in front of others to be authenticated.
End-user information and communications are encrypted and securely stored.

**Privacy compliant**
Privacy is inherent to Natural Security. The technology prevents tracking of individual users, for example when they enter a store. It does not use databases; instead, biometric information is securely stored on the consumer device itself, under the individual user’s control at all times.
Use cases

Natural Security is designed for situations where verification of individuals is critical, especially for payment operations and to control access to premises or Internet resources.

Banks can implement Natural Security to protect and simplify the various points of contact with customers, while capitalizing on the trusted relationships already established with these customers. In retail, it can be used to improve customer experience and leverage synergies between different distribution channels.

Other companies can use Natural Security to control access to physical and information resources without any inconvenience for employees.

Payment

The use of biometrics guarantees that the device and its owner are at the same place at the same time. The voluntary action involved—controlled entirely by the owner, made of his own volition, and requiring his physical presence—resolves the problems caused by loss or theft of a means of payment, all the while ensuring transactions cannot be repudiated.

In addition, because Natural Security relies on contactless technology, it spares users the need to physically handle the device, thereby optimizing payment operations both in stores and online.

Physical and logical access control

When used for access control, Natural Security provides an additional level of security and simplifies the ergonomics involved in authenticating employees. It enables companies that use access cards to enhance protection of sensitive zones by locally deploying biometric readers without having to completely change their infrastructure. For companies that already use a biometric system linked to a database, this technology increases security by requiring the presence of three factors (the personal device, the device owner and an optional code). The transaction is executed using mid-range contactless technology combined with biometric user authentication.

Natural Security comes in response to the increasing number of IDs and passwords required to access remote services such as online banking, email accounts and social networks. It simplifies services requiring authentication while increasing security by requiring the presence of both the individual and the data on the personal device.
Natural Security aspires to be synonymous with speed and security for service providers, banks and shops while at the same time guaranteeing both the protection and privacy of personal data for end users.

Click & Mortar
Natural Security as a business enabler

For issuers
Natural Security is the best way for issuers to monetize one of their most important assets: KYC (Know Your Customer) by guaranteeing the identity of the user on every channel.

For merchants
Natural Security improves customer experience with a convenient and fast way to pay, to sign and benefits from customer authentication whatever distribution channels (internet, shops).
For payment, the use of biometrics guarantees that the device and its owner are at the same place at the same time. The voluntary action involved – controlled entirely by the owner, made of his own volition, and requiring his physical presence – resolves the problems caused by the loss or theft of a means of payment, all the while ensuring transactions cannot be repudiated.

For service providers
Natural Security brings to the market a high level of security combined with a fast and convenient way to authenticate a customer.

For banks
Banks can implement Natural Security to protect and simplify the various points of contact with customers (ATM, internet, branch offices) while capitalizing on the trusted relationships already established with these customers.

For corporate usage
Natural Security allows to control access to physical and information resources without any inconvenience for employees. Natural Security provides an additional level of security and simplifies the ergonomics involved in authenticating employees.

For manufacturers
Natural Security develops an authentication standard for the industry based on requirements from issuers, banks, retailers and service providers.
Financed by companies in the retail, banking and industrial sectors, Natural Security reflects the business needs associated with the use of biometrics to protect transactions and access services.

Natural Security develops and maintains the specifications for its strong authentication standard, which are available through licenses to all industrial organizations and users interested in developing solutions.

These specifications provide background details on the technology, descriptions of individual implementations (in particular, the type of biometrics and secure element used) and evaluations. In this way, Natural Security can recommend the most suitable technology for different use cases. Natural Security provides leading-edge solutions for key global sectors, including the payment, banking and retail industries.

Stakeholders include banks (Banque Accord, BNP Paribas, Crédit Agricole, Crédit Mutuel Arkéa), retailers (Auchan, Leroy Merlin) and a manufacturer (Ingenico).

Natural Security has defined the four conditions it considers crucial to developing a consumer market for 2 factors authentication based on biometrics:

1. An evaluation of the different biometric technologies conducted in real-life situations rather than in laboratories, such as the one performed by the Biometrics Alliance Initiative. This type of evaluation, which looks at security, performance and usability, is designed to assess biometric technologies according to the same criteria as other technologies used in the banking industry. Natural Security is a founding member of Biometrics Initiative Alliance.

2. Storage of authentication data and applications on a personal device that, in addition to providing better protection, can be used in various situations and environments. This facilitates the development of new usage, which companies can then adopt to expand their business model;

3. Definition of a quality mark to educate final users and bolster confidence;

4. A privacy by design approach that addresses personal data protection and privacy issues prior to the design phase.

About Natural Security

Core Values
Milestones

2006  Project started by banks and retailers
2008  Company creation. General availability of the first version of the specs, first proofs of concept
2010  NetExplorateur Award 2011
2011-2012 Launch of the commercial phase
       Several pilots planned in 2012: payment (open and close loop), access control (physical and logical), mobile payment
       Development of industrial «off-the-shelf» NS products

Awards :
• Technology award 2010 – Publi-News
• NetExplorateur 2011
• Innovative Payments award 2011 – Publi-News
• “Grand Prix Entreprises et Cités” 2011 – «Société Industrielle du Nord»
• Nominee for the Florin Transaction Services Innovation Award 2012

NS community

Natural Security defined the specifications for a strong authentication system that relies on a contactless secure element and biometrics. This system quickly, ergonomically and securely authenticates users for payment transactions, electronic signatures and access to services. Use of a personal device ensures that the final user’s personal data and privacy are protected, while facilitating authentication in different contexts, including at home, at the store, in a bank or at an ATM or vending machine.

As part of the development process, Natural Security wanted to create a «Natural Security community» where its members could discuss the solution and the various ways in which it can be used.

The community is designed to bring together the different parties involved in building the Natural Security ecosystem. These members include companies that use the solution (e.g. retailers, banks, service companies), industrial companies and integrators, as well as experts and associations interested in understanding the relevant issues and helping deploy Natural Security’s concepts and technologies.
The Biometrics Alliance Initiative, which has its roots in the observation shared by current and potential users that biometric technologies are difficult to evaluate, held its first working conference on February 1, 2012.

The lack of both a recognized certification process for biometric technologies and a harmonized European standard directly impacts the confidence users have in this type of technology. Even though standards already exist to ensure biometric systems are interoperable (especially government applications), widespread adoption of these standards for commercial applications and within companies would require the creation of suitable frameworks for evaluating the performance, security and usability of such systems.

Not all biometric technologies or their implementations are created equal: some are built for convenience whereas others are designed to reinforce security. By characterizing, classifying and evaluating biometric systems, whether in relation to usage contexts or not, stakeholders can help users learn, and continue, to trust biometrics.

The Biometrics Alliance Initiative was created to fulfill this need to establish security, usability and performance measures and standards for biometric technologies. It aims to define a testing, certification and accreditation process, including testing procedures, to ensure biometric solutions provide a level of security that both meets the needs in question and complies with international standards, especially banking standards.

The objective is to provide Biometrics Alliance Initiative members with the building blocks for a framework that can be used to evaluate biometric technologies. As such, the organization is working to express and formalize user needs, as well as to provide concrete operational recommendations for parties involved in developing biometric solutions. For biometric companies, then, the Biometrics Alliance Initiative provides a means of both formally identifying user needs and business requirements, and establishing a transparent evaluation methodology that relies on objective criteria and does not hamper competition.

The Biometrics Alliance Initiative is ultimately looking to establish an industry standard to benefit as many different parties concerned by the use of biometric technologies as possible. A significant number of stakeholders have already taken an interest in this initiative, including government bodies, the banking industry and individual companies.

Founders and members of the Biometric Alliance Initiative include Banque Accord, the Innovation Centre of Contactless Technologies (CITC EuraRFID), Ensicaen, Leroy Merlin, Natural Security, Paycert, TazTag, Underwriters Laboratories (UL), Vauban Systems and Wincor-Nixdorf.
Please send a mail to

contact@naturalsecurity.com

or visit us on

www.naturalsecurity.com