



F R O S T & S U L L I V A N

50 Years of Growth, Innovation and Leadership

How to Win Your Anti-Counterfeiting War

A Frost & Sullivan
White Paper

www.frost.com

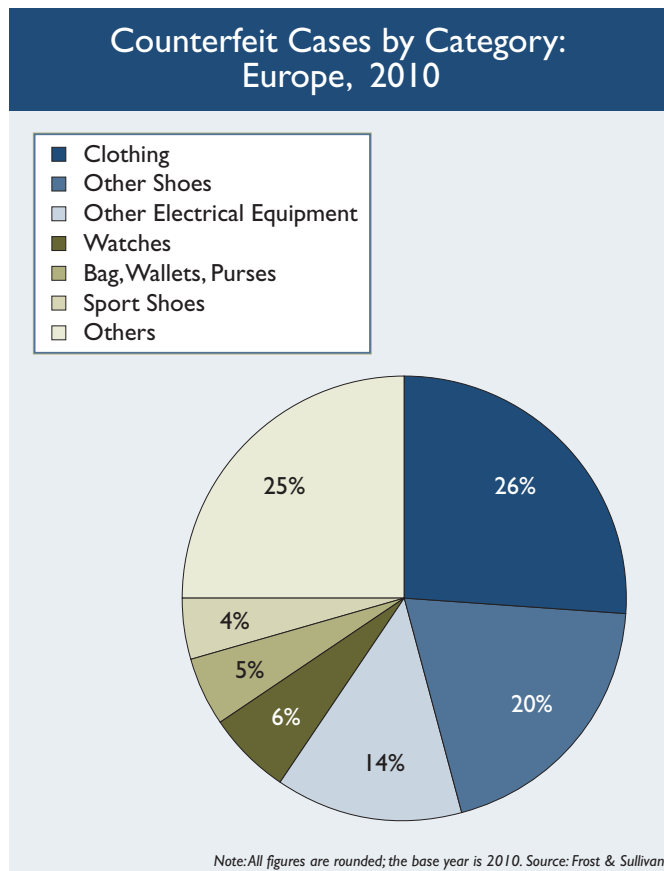
Counterfeiting: Global Context.....	3
<i>Global Situation</i>	<i>3</i>
<i>Brand and Intellectual Property Protection</i>	<i>4</i>
<i>New Threats and Impacts per Vertical</i>	<i>5</i>
What are the Available Solutions to Prevent Counterfeiting?	7
<i>Traditional Solutions Approach</i>	<i>7</i>
<i>Advanced Technical Solutions</i>	<i>8</i>
Best Practices to Implement Anti-Counterfeiting Measures	10
<i>Cost Impacts and Rationalization</i>	<i>10</i>
<i>Technical and Energy Impacts</i>	<i>11</i>
<i>Market Differentiation (Quality, Safety, Authenticity)</i>	<i>11</i>
<i>Business Differentiation (End User approach, Instant Answer, Brand Transparency)</i>	<i>12</i>
Is VaultIC the Best Solution for Anti-Counterfeiting?	13
<i>What is it?</i>	<i>13</i>
<i>Where is the Value Added?</i>	<i>14</i>
Conclusions	16

COUNTERFEITING: GLOBAL CONTEXT

Global Situation

With the explosion of the globalization economic model, brands become increasingly important. It is a particularly relevant trend for luxury goods, but also for all other high-end products. Companies have invested a lot of money in brand recognition and value as a key area of differentiation. This investment is important and strategic as it is directly linked with end users' perception, which is key with regards to new marketing models. Indeed, direct marketing strategies allow companies to communicate directly with their client, and to some extent integrate them as part of the brand.

Counterfeiting, or the practice of copying a genuine product and creating a fake version, is a threat for the industry. According to the International Anti Counterfeiting Coalition (IACC), \$600 billion is lost each year due to counterfeiting. According to the U.S. Chamber of Commerce, this threat costs up to \$250 billion a year in the U.S. alone, with up to 750,000 jobs adversely impacted as a result. The story is similar in Europe. According to the European Commission, cases involving IPR (Intellectual Property Rights) infringements almost doubled to nearly 80,000 in 2010, representing goods where the estimated value of the equivalent genuine products was more than Euro 1 billion. In 2010, a spectacular increase was seen for luxury goods and electronic devices.



Brand and Intellectual Property Protection

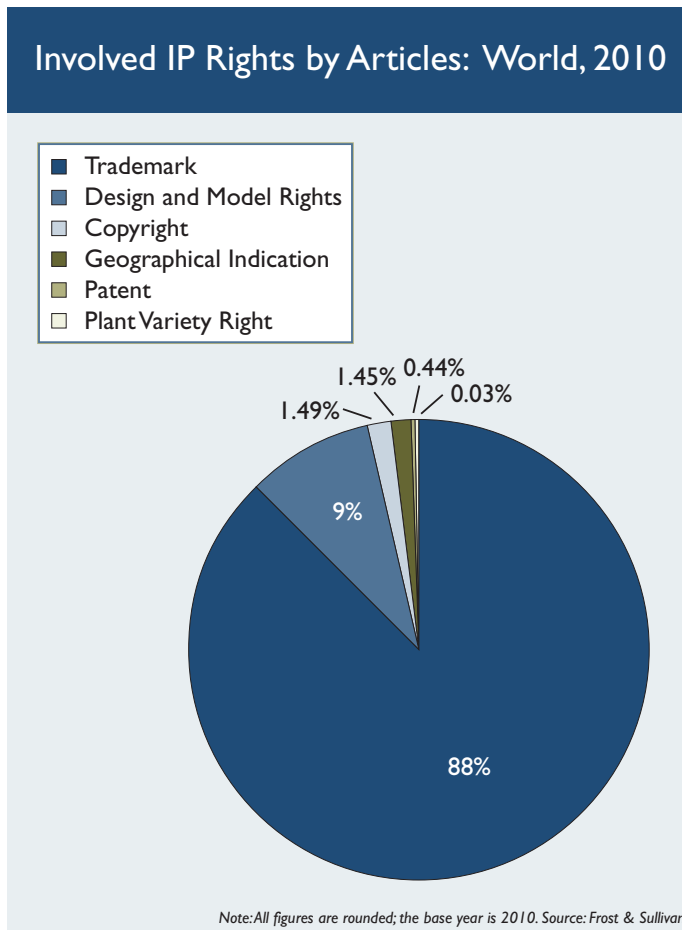
The World Intellectual Property Organization (WIPO) defines Intellectual Property and Intellectual

Property Rights as follows:

Intellectual property refers to creations of the mind. It is divided into two categories:

- Industrial property includes patents for inventions, trademarks, industrial designs, integrated circuits, and geographical indications.
- Copyright and related rights cover literary and artistic creation.

Intellectual Property Rights allow the creators—or owners of patents, trademarks or copyrighted work—to benefit from their own work or investment in a creation. These rights are outlined in Article 27 of the Universal Declaration of Human Rights, which provides for the right to benefit from the protection of moral and material interests resulting from authorship of any scientific, literary or artistic work.



IPR is one of the most challenging issues facing the Information Technology (IT) industry. The black market (i.e., supplying non-genuine goods within an illegal distribution channel) and also the development of the gray market (i.e., using an illegal replica within the official distribution channel and partners) have a direct financial impact by cutting sales revenues. This threat definitively impacts investments in research and development (R&D). An estimated 10 percent of high-tech devices sold worldwide today is counterfeit.

The impact of the gray market is huge. As mentioned, companies have invested heavily to promote their brands and to reach a high level of quality in terms of product, services and customer support. Such threats dramatically decrease the positive perception of the brand by end-user consumers.

In mid-2010, it was reported that five unregistered Apple stores had been discovered by an American woman living in Kunming, China. These unofficial stores were very similar in appearance to official stores. Each detail (including staircase design, seating area and chairs, employee T-shirts and ID lanyards, etc.) were copied from the U.S.-based brand. Official Apple products were available in these stores. Apple did not comment on the discovery of fake shops, but since July 2011, two of these stores have been closed as their owners were unable to provide a business license.



Source: *bird abroad*

New Threats and Impacts per Vertical

According to the Alliance for Gray Market and counterfeiting Abatement (AGMA), "It is estimated that over \$40 billion in legitimate products move through the gray market each year, resulting in \$5 billion in lost profits annually to manufacturers." For more than 10 years in Europe, the numbers of cases have grown rapidly to reach more than 79,000 relevant cases in 2010, accounting for up to 103 million products. As is often the case in Europe, most of IPR infringing goods were cigarettes, but high-tech and luxury goods are increasingly affected.

Each country has tried to find ways to protect their brands; in France, The Union des Fabricants (UNIFAB) announced that the number of counterfeit mobile handsets increased by 57 percent between 2005 and 2006. This is an important target market for the counterfeiting industry. There are so many copycat mobile handsets on the market coming from Asia—and especially China—that a new word has even been created: “Shanzhai.”

This counterfeit offer is much more than only a passing trend. This is an organized industry featuring a large ecosystem of players. Counterfeiters were even able to deliver fake iPhones in 2005, notably CECT’s P168 device. In 2011, it was reported that Dhanji Damor, a 25-year-old man from the Panchmahal district of Gujarat India, received an electric shock from his fake mobile phone while attempting to make a call and while his mobile handset was plugged in for recharging. This story, if confirmed, is a strong signal to developed countries. Indeed, it is crucial for the industry to clearly fight against fake mobile devices. This is a question of life and death; the lack of reliable technology can be dangerous and even mortal.

iPhone: Original and Fake Version



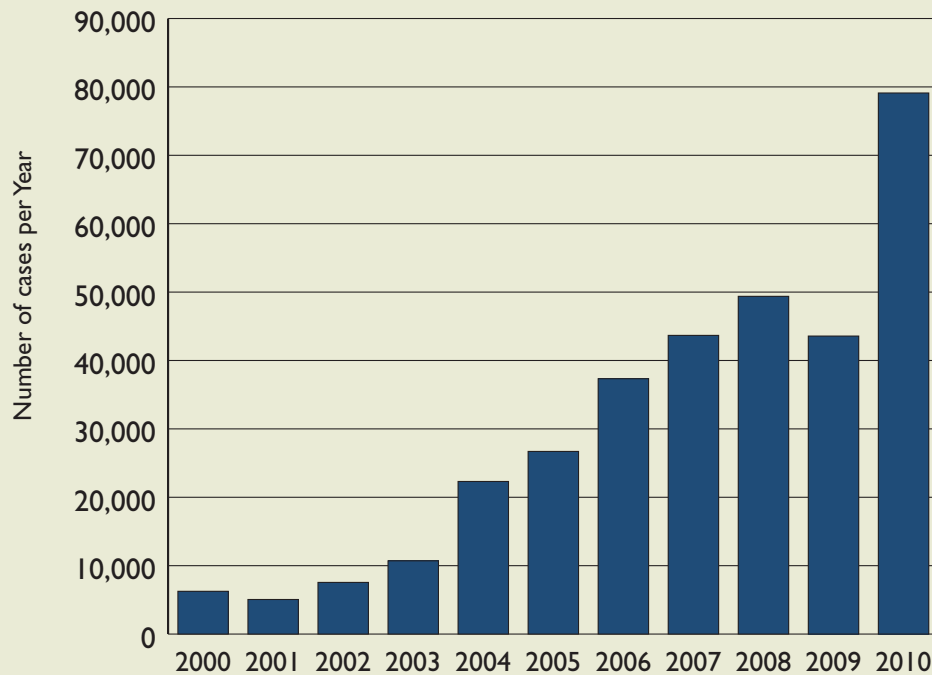
Original



Fake

Luxury goods are also facing this threat. In France, the industry is facing a direct negative impact in terms of revenue of between 4 percent and 7 percent due to counterfeiting. All subsectors are impacted. In 2000, a study published by the Global Anti-counterfeiting Group (GACG) concluded that the cosmetic and perfume industry was losing about 555 million Euros each year to counterfeiting. Branding is a crucial strategy in the luxury industry. Counterfeiting is a problem for such companies as they need to face potential end-user dissatisfaction due to the impact of fake products. The Organization for Economic Co-operation and Development (OECD) estimated that the perfume industry has to deal with a 5 percent sales loss every year due to counterfeit product.

Number of Cases per Year: Europe



Note: All figures are rounded; the base year is 2010. Source: Frost & Sullivan

WHAT ARE THE AVAILABLE SOLUTIONS TO PREVENT COUNTERFEITING?

Worldwide financial losses due to counterfeiting have been rising rapidly over the course of the past decade. In this industry, anti-counterfeiting initiatives are much more than a solution to win the war; they are solutions directly included in the products themselves. This is particularly true for both banknotes and traveler's checks, where the industry continues to innovate in the battle against counterfeiting. National printing companies who provide official documents such as national ID cards, certificates and documents regarding ownership are also leading research for innovative and efficient anti-counterfeiting solutions.

Traditional Solutions Approach

The first requirement in the fight against counterfeiting is to find an easy way to check if a product is genuine. This check has to be quick and without the need for a considerable amount of technical interaction.

- **A holographic approach** is one of the most effective solutions to enable visible inspection. The end user is able to check that certain visible features are present on the product. Holograms are commonly described as an “advanced-printing technique which creates the illusion of three dimensions on a flat (e.g., two-dimensional) surface.” This is a well-known and developed technology, but unfortunately not so easy to verify (as final users are not aware of the details that need to be checked) and, unfortunately, counterfeitable. More advanced holographic technologies are available to account for the fact that holograms are inert and hence easy to copy due to the fact also that the hologram is physically accessible. For example, existing solutions allow the hologram itself to react to stimuli (physical, chemical or electrical). However, this is not the best solution for top high-end products as the level of protection is poor compared to the price of the device itself.
- **Bar codes** are also used to protect genuine goods. A bar code is a small image of lines and spaces that is affixed to retail store items to identify a particular product number or any other requested information. Last technologies included a matrix bar code (2D bar code) instead of a linear bar code. This is an easy solution to deploy, but once again, end users are not able to check if the product is a fake one without a special reader. The fact that the readable information is, most of the time, written in clear in the bar code is not a completely secure solution. Nevertheless, it is true to say that bar codes were originally created for product tracking only, not anti-counterfeiting. The pharmaceutical industry uses this technology to aid product traceability and fight counterfeiting. This is a good opportunity for this industry as bar codes can be printed or stuck directly onto the box or master cartons. But this is less relevant for luxury goods or high-end tech goods, where the product should be identified individually, without certified packaging.
- **The compilation of several secured solutions** is one of the best approaches. Indeed, complex image printing coupled with advanced ink solutions offers much more than simply a secure solution. Technical features such as Intaglio printing, watermarks, micro printing, infra red, magnetic and ultra violet are widely used for the fight against currency counterfeiting. This range of security solutions protects official documents and banknotes from standard counterfeiting. But this is a costly solution due to the manufacturing process that needs to be engaged and is not fully relevant for the luxury goods and high-tech sectors. Indeed, such solutions are not widely used for these products as printing directly on goods is seen as an inappropriate solution.

Advanced Technical Solutions

All previously discussed solutions are really easy to use. This is positive in terms of the ability to provide visual verification, but it also has inherent security weaknesses. To protect goods against this menace, the electronics industry has

developed electrical and electronic devices to help with anti-counterfeiting measures. While the original purpose of bar codes was to track and identify goods, newer solutions also deliver anti-counterfeiting capabilities.

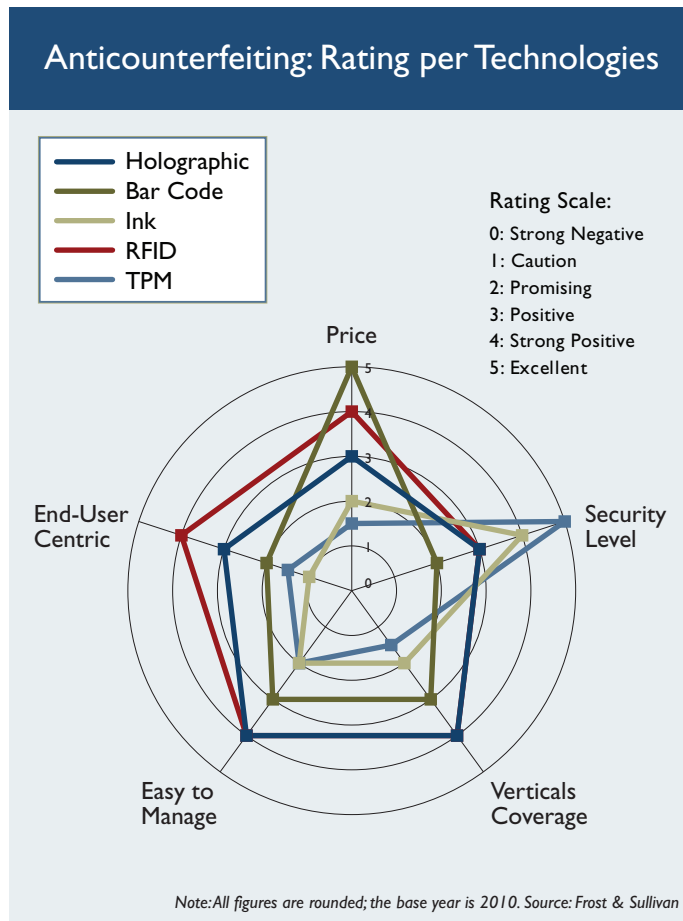
RFID tag



- One of the first technical answers was the RFID tag. A RFID chip or tag is a passive antenna that can be activated when it is close to an energy source. When the RFID device is scanned by a reader, the chip delivers a set of data that can be verified against a database. The real value of such a device is to have a low price (from a few cents up to \$1) for standard product. This is a simple solution that is easy to install and well known by customers. The primary use of this solution is to track products across the logistics chain. New applications have been used since the introduction of RFID tags for anti-counterfeiting purposes. The idea is to check, during the RFID tag reading process, that the information contained on the chip is the same as that stored in a centralized database. If it matches, then the product is a genuine one. But this is not a fully secure process. Indeed, several articles and demonstrations have revealed that it is possible to view the memory content of the RFID tag. It is then a rather simple task to create a new RFID tag containing exactly the same data information. More complex RFID tags are available and are based on Physical Unclonable Functions (PUF). But the price, the real value added of the tags, is definitively less competitive due to the addition of new security features.



- Trusted Platform Module (TPM) is arguably the most advanced technical solution, but also the most expensive and the most binding one. Indeed, for high-tech goods, genuine verification or to protect IP, TPM solutions are often used. The solution includes a secure cryptoprocessor embedded directly into the high-tech goods (most of the time for computing devices). This embedded and specialized chip is able to contain secrets, digital certificates, encrypted keys and even passwords. It allows the hardware itself to be identified, but also handles Digital Rights Management (DRM) as well as software license copyright. However, the price is quite high, so the use is most commonly linked with high-end technical products. In 2010, TPM was cracked after a long and difficult process during a demonstration in Black Hat DC Conference. There is no long-term, fully secured solution, but the final use should strike a balance between price, security and ease of custom.



BEST PRACTICES TO IMPLEMENT ANTI-COUNTERFEITING MEASURES

Cost Impacts and Rationalization

According to the EGA (European Generic medicines Association), the cost of anti-counterfeiting projects to track and trace medicine to fight against counterfeiting is approximately €400 million per single supply chain. For the EU-25, this amounts to a total investment of about €10 billion, combined with an estimated annual €500 million for operational costs. This cost is only associated to project deployment, with extra costs potentially with the chosen technology. This approach is not only linked with the medicine anti-counterfeiting war—it is also the case for luxury goods and electronic devices. Such strategies should be rationalized to avoid any extra cost. This is particularly true in a global context. Indeed, it is important to follow international rules and even sometimes local or regional rules. Counterfeiting definitions and punishments can be drastically different between regions. Even if an economical zone agreed on a common approach with a governmental or industry organization, a global approach is not well defined at this time. This is why those

companies directly impacted with counterfeiting threats should handle their own solutions to be able to meet their specific challenges. The complete system should be evaluated from the perspective of the anti-counterfeiting device itself, the reader, the required infrastructure (computers, network, database, etc.), and the reliability of the dedicated system (such as read rates).

Technical and Energy Impacts

A global technical approach is the most important element of the implementation of an anti-counterfeiting project to optimize cost rationalization. To ensure an efficient solution, the technical choice should focus on the certification and standardization capabilities. It is crucial to have a well-established system and processes to anticipate—and even avoid—future problems. The most common strategy is to add a new technical solution with a focus on price and easy installation. Once completed, the value added is rarely easily visible. Some problems could appear due to regional or other specificities. This is the case, for example, for RFID tag solutions; such solutions could face reading issues. In practice, the successful read rates for such solutions reach only 80 percent due to radio wave attenuation. In conclusion, the solution should have the capability to be reliable, standardized and certified everywhere across the globe.

Finally, the technical choice should answer these questions:

- Is it a cost-effective solution compared to the threat?
- Is it a technical solution easy to deploy and available worldwide, certified and reliable?
- Can the solution be verified as genuine everywhere, by everybody and at any time without any complex process?

Market Differentiation (Quality, Safety, Authenticity)

More than 75 percent of companies that have faced counterfeiting issues mentioned that their brand perception is hugely impacted. Nevertheless, with the same anti-counterfeiting strategy, companies could potentially reduce revenue loss and also protect their brands. Indeed, companies need to benchmark their exposure to the black and gray markets and then design an adapted solution to the potential threat. Of course, this is an opportunity to provide a clear message to the market, and to be seen as a market leader. End users need to trust a product and then trust a brand. To do so, the company should be able to guarantee the product quality, safety and authenticity.

As a global regulation and anti-counterfeiting law will take time to be created and applied, each company should assume responsibility for protecting their own market and products. This is an important message for the client and a real differentiator in terms of quality.



The strategy could be summarized as follows:

1. **Benchmark** the risk, the exposure, the cost
2. **Choice** of an efficient and relevant technical solution
3. **Deployment** of the global solution
4. **Control** and monitoring of the anti-counterfeiting measures in real time
5. **Optimize** part of the process to adapt the solution to the threat if needed

Business Differentiation (End User approach, Instant Answer, Brand Transparency)

Over the course of the past decade, a new consumer generation has emerged. This generation demands direct interaction with their favorite brands, an extremely personalized product, and a social network to reflect their interests and lifestyles. This is the result of the Internet experience and new communication media such as mobile handset and, above all, smartphones. Companies are investing heavily to try to implement adequate brand strategies. This is an answer to client desires and a real differentiator to the competition. This new end-user approach allows companies to deliver a message to their final client; a message focused on the fact that the client is part of the brand and the brand a part of the client. This is a new component of the marketing strategy and a positive signal to the connected generation. Indeed, brands that invest in this direction are likely to create not only a great buzz, but also a completely new level of loyalty from their customers.



Source: Frost & Sullivan & Social Media Prisma

Anti-counterfeiting is a part of this global strategy. This is a tremendous opportunity for any company to demonstrate to their clients that they are investing money and time to deliver the best possible quality of service and goods. Of course, end users are not naïve, and they have a critical perception of marketing or advertizing messages. This is amplified by communication across social networks. Finally, end users need to believe and rely on the brand to have a brand transparency understanding. Anti-counterfeiting solutions should answer these requirements and be able to have an instant answer. Each company should be able to provide high-end goods and services and to answer these expectations every time and in every customer interaction.

IS VAULTIC THE BEST SOLUTION FOR ANTI-COUNTERFEITING?

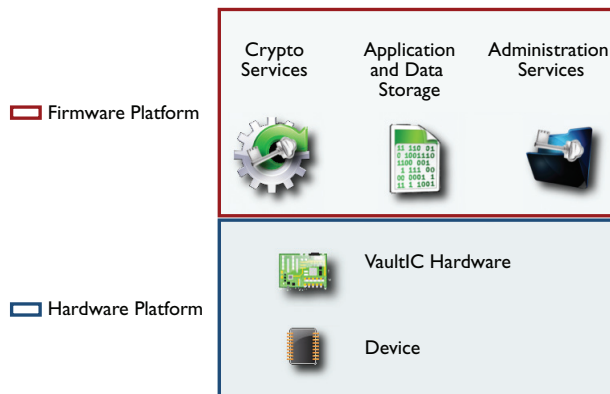
To optimize your anti-counterfeiting strategy you need to follow several steps. This section considers the extent to which Inside Secure’s VaultIC device can offer a solution in the war against counterfeiting.

What is it?

Instead of using a complete software solution, or even worse to develop personalized software for anti-counterfeiting measures, VaultIC is an electronic device—more specifically, it is a secure micro controller. This is an independent device solution with a complete firmware dedicated to IP protection, anti-cloning and identity theft. The device is based on banking and smart cards product hardware, so it has a foundation based on high-level security mechanisms and reliability.

VaultIC can be defined as a combination of two different platforms.

- The “hardware platform,” with the device and the VaultIC hardware (memory section, CPU, crypto engine, hardware security, power management, etc.)
- The “firmware platform,” with Crypto Services, Application Management and Data Storage, Administration Services



To enable access to the external world, the last levels are an application interface and a security domain.

Where is the Value Added?

- Security level and particularities

This secure micro controller is fully certified by the Common Criteria Certification, with the top level of EAL5+. It guarantees that the device itself had been designed, developed and tested to reach this security standard.

The firmware also received the top level FIPS 140-2 Security Level 3 for the first time for such a product. This certification is based upon NIST standards, and U.S. and Canadian certifications for cryptography security level. It certifies that the component cannot only securely generate data, cryptogram and signature, but also detect and overpass possible physical attacks.

The crypto services module is based on the last cryptography recommendations (with asymmetric cryptography) for keys and certificates generation. VaultIC features authentication with the use of Elliptic Curves technologies, which makes the solution more robust. Indeed, the Elliptic Curve Digital Signature Algorithm (ECDSA) is a technical choice that delivers faster key generation as the key is smaller than standard DSA and RSA keys, albeit with the same levels of security.

The micro controller can also be used for a more secure solution with the addition of Public Key Infrastructure (PKI).

- Cost effective, complete solution, module approach

The anti-counterfeiting war is only a small part of the total price of a product. After a benchmark between the cost of a threat and the anti-counterfeiting measures, the main driver will be the cost. VaultIC is a very low-cost solution with high security levels and standards. In addition, the device could be easily included in all packages and goods as it is available on a DFN6 form factor.

With the secure micro controller, a complete package offer could be proposed. But this package targets a flexible approach and a module approach to address on-demand client needs only.

It starts with a personalization offer, if needed. It means that the commercial offer could include a manufacturing process with data generation for the key management, for example, or interaction with certificates authorities. It is also possible to be assisted with database creation, for certificate storage and/or the integration of these certificates in an existing internal solution. At the end, personalized applications could be proposed for an “easy-to-use” control of the genuine device. But all these services are offered as options, so finally a module and flexible approach for client satisfaction.

- Energy consumption, product lifetime and management

VaultIC is a low-cost device offering high levels of security. In addition, the secure micro controller has low power consumption linked with a small footprint and is available with a very low pin count. This is an easy solution to integrate in goods. Most of the time, embedded devices do not have a dynamic life cycle. Put simply, after the personalization itself (embedded certificates, embedded signatures, etc.) there is no way to interact with the device to modify its behavior with the external world.

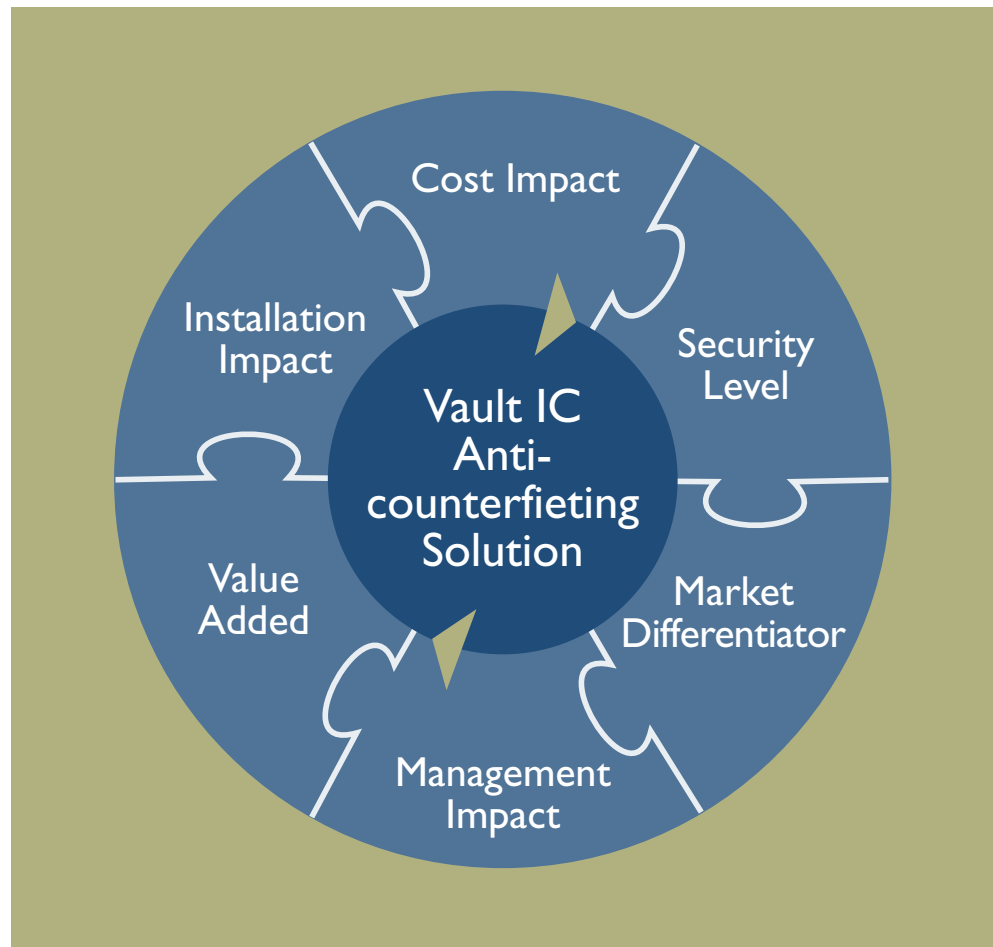
Such capabilities offer a strong advantage as VaultIC can be adapted to numerous situations. During a reading session with a tag including VaultIC, it is possible to send proprietary commands to change device status. For example, this could be done to put the device in a terminated state during a reading session. It means, for example, that the verified good is a fake one. So the secure micro controller should be put in a terminated status and the database updated to identify the counterfeit product and avoid any future problem.

- End user experience

This is definitely the most important element of VaultIC's differentiation. To be able to fight against the gray market, the best solution is to involve the end-user customer directly. There is a double advantage in this solution. The company, so the brand, is transparent and makes the client the major actor of the anti-counterfeiting strategy.

VaultIC is a solution that allows control and check by using a smartphone and a dedicated application. The NFC (Near Field Communication)-based solution is a technology that offers a short range and contactless communication between two devices. If the NFC technology in a smartphone can be coupled with a dedicated and simple application, it is easy to imagine that a complete and secure solution to control and validate that a good is genuine can be delivered. This is a real-time answer and an instant service for the client.

For the end user, it is an innovative and interesting experience. For the first time, he will be deeply associated to his favorite brand. And for the company, it is a wonderful marketing solution to have a dedicated and personalized application to assist their client in the anti-counterfeiting fight that also offers the potential to promote and propose loyalty rewards.



CONCLUSIONS

There is no more protected market to counterfeiting. Luxury goods, traditionally complex and difficult to copy, but also high-tech goods are also targeted goods for the black and gray markets.

When there is a risk regarding safety, liability or health, it is vital to engage a strong and total war against the counterfeit market. And what is logical for goods is also true for intellectual properties rights.

Finally, each company and every brand should be prepared for this fight. To reach this objective, a tactical battle plan should be developed. A sharp analysis of the threat, the risk and the cost will naturally drive the company to choose a secure and reliable solution. Indeed, time is coming to make the balance between the cost of the threat, the impact on the brand, and finally on end-user brand perception.

Instead of using the anti-counterfeiting solution as a new cost center, companies should take the opportunity to propose a market differentiator and to offer their clients a new experience. The end user is becoming one of the most relevant parts of the brand. This is particularly true with the rapid deployment of social shopping and the huge strength influencing force of social media.

According to Frost & Sullivan, the most advanced solution will be an embedded solution, including last-certified and standardized security features. But the anti-counterfeiting solution should be also flexible to allow the company to decide what part of the logistic chain should be involved. Finally, contactless features such as NFC will allow the brand to experiment with a new customer communication dimension. The final verification check will be handled in real time by the end user with a simple mobile phone for every product, everywhere and at any time.

It is important for the industry to always be one step ahead of the black and gray markets, and embedded solutions with contactless capabilities are keys to winning this war. But the industry should also be ready for the next threat across the e-commerce industry and virtual shops. Anti-counterfeiting providers will have to find new ways to avert this new danger. Finally, it is another war to fight.

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10,
Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SW1W 0DH, UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
<http://www.frost.com>

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company's TEAM Research, Growth Consulting, and Growth Team Membership™ empower clients to create a growth-focused culture that generates, evaluates, and implements effective growth strategies. Frost & Sullivan employs over 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from more than 40 offices on six continents. For more information about Frost & Sullivan's Growth Partnership Services, visit <http://www.frost.com>.

For information regarding permission, write:

Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041

Auckland	Dubai	Mumbai	Sophia Antipolis
Bangkok	Frankfurt	Manhattan	Sydney
Beijing	Hong Kong	Oxford	Taipei
Bengaluru	Istanbul	Paris	Tel Aviv
Bogotá	Jakarta	Rockville Centre	Tokyo
Buenos Aires	Kolkata	San Antonio	Toronto
Cape Town	Kuala Lumpur	São Paulo	Warsaw
Chennai	London	Seoul	Washington, DC
Colombo	Mexico City	Shanghai	
Delhi / NCR	Milan	Silicon Valley	
Dhaka	Moscow	Singapore	