EUROSMART
The Voice of the Smart Security Industry

VISION 2020

PROVIDING TRUST AND SECURITY IN A HYPERCONNECTED WORLD

November 2014

FOREWORD

Which digital identities will you have in the hyperconnected world of 2020? How will cloud services streamline digital services and contribute to a better quality of life? How can you be confident that the cashless payments you make do not compromise your banking data? And finally, while the many connected objects you will own add convenience, what about security and privacy implications? This Vision 2020 paper by the smart security industry takes a peek into the future for possible answers to these important questions.

The digitalisation of our world, which goes hand in hand with the globalisation of trade and services, is the hallmark of the 21st century. Smart devices are getting ever smaller, user convenience is improving rapidly, and people can access digital services from even the remotest corners of the world. The vision of a world where everything and everyone is connected at all times, independent of time and location, seems on the verge of finally becoming reality. The Word Economic Forum (WEF) calls this phenomenon "hyperconnectivity" and estimates that by 2020 "50 billion networked devices will underpin our societies and economies". With technological innovations such as SIM cards, secure payment and electronic ID cards as well as associated solutions and services, the smart security industry is one of the major players at the heart of this development, both driving its evolution as well as safeguarding it against fraud and violation of privacy.

While a hyperconnected world may offer huge opportunities and benefits for human society, the WEF points out the risks associated with it:

> ***Hyperconnectivity could exacerbate inequality in the world, both through differing access to digital technology as well as rapid changes in skills required to survive and thrive. Hyperconnectivity is also creating a new level of security risks.***
> ***(World Economic Forum)***

The smart security industry shares this assessment. And while we regard the first risk, increasing inequality, as a grave one, we are not in a position to mitigate it. This is the task of policy-makers and public institutions. We are, however, uniquely equipped to provide solutions for the second risk, security. Eurosmart members design products, solutions and services that are based on the secure element concept.

> ***Secure Elements embed a secure microcontroller that is both a "safety deposit box" of data and processes and the support base of embedded software that is protected against viruses, malware and Trojan horses. Since they are mostly personal and portable, they are under the individual control of each user. (Eurosmart)***

It has long been the smart security industry's credo that trust is at the core of successful connections. Trust starts with an assurance that the person or entity you deal with is indeed who they claim to be. In the digital world we can achieve this with strong authentication solutions. By securely storing the credentials used to prove digital identities in a tamper-proof secure element, physically under the sole control of each individual, trustworthy transactions can take place.

As the Voice of the smart security industry, Eurosmart will continue to promote smart security solutions that aim to improve the usability of digital services while protecting privacy and combating fraud. Eurosmart will renew its efforts to educate the public about potential dangers and what they, as responsible users, can do to prevent or at least minimise security risks.

This Vision 2020 paper is one contribution towards this goal, and presents our proposals on how to better tackle security incidents, fraud and data breaches in the fields of digital identities, payments and connected objects

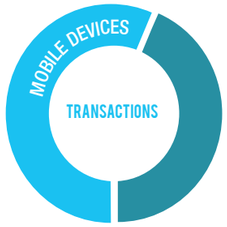
THE CONNECTED WORLD IN 2020

WHAT IS A SECURE ELEMENT?

A SECURE ELEMENT contains a **secure, certified** microcontroller and embedded software.
It is secure, personal and portable and comes in **multiple form factors.**
It is **vital** to ensure digital security and privacy.

Close to **50%** of the forecasted global population will have access to internet (McKinsey)

SMARTPHONES will account for **2/3** of every mobile connections globally (GSMA)



More than **50%** of transactions will be made by **MOBILE DEVICES** (VISA EUROPE)

Smart watches in-use to reach over **100 MILLION** (JUNIPER RESEARCH)

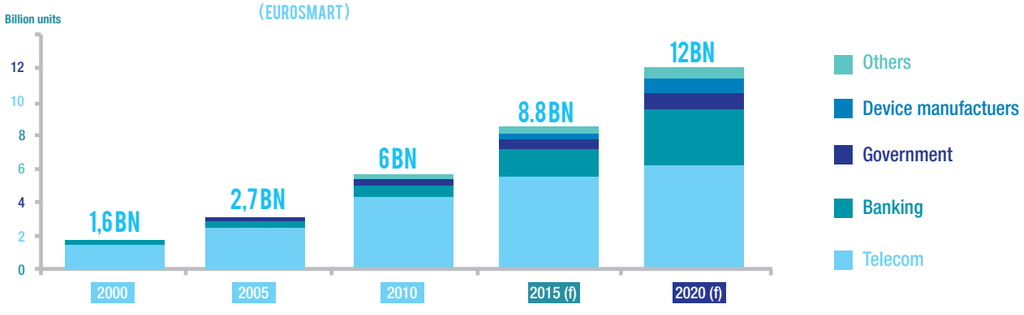
(TELEFONICA)
90% of cars will be connected

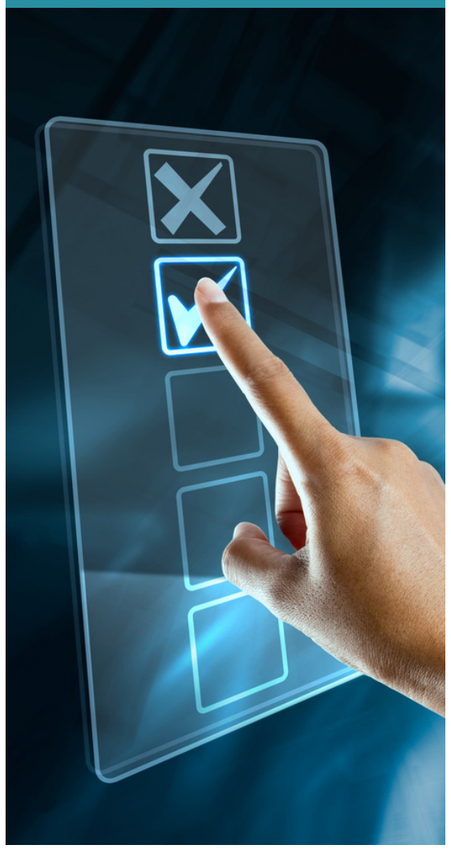
HALF THE WORLD
will have National eID Cards
(ACUITY MARKET INTELLIGENCE)

1,2 BILLION mobile phones sold in 2018 will include **NFC TECHNOLOGY**
(IHS TECHNOLOGY)

SECURE ELEMENTS SHIPMENTS ESTIMATES UNTIL 2020

(EUROSMART)





IMAGINE A TYPICAL GOOD DAY IN 2020 FOR LUKAS, A DIGITAL CITIZEN

Lukas wakes up at the right time thanks to a sleep monitoring app on his smartphone. At a glance he gets the current information he needs: messages from his parents and best friends, local weather, traffic on the way to his office, sports results for his favourite team, news on his topics of interest. Automatically, the coffee is ready, TV or radio is on, and the lights are switched off when he leaves the apartment.

The journey to the office is relaxed thanks to his autonomous car. He is authorised to enter the corporate building through a biometrics verification coupled to his smartwatch. He has an important customer meeting. He shares some confidential files in real time with other colleagues; the result is immediately available for all authorised people, wherever they are in the world, whatever the device they are using.

He receives a notification from his doctor that he needs to perform a glucose test. He does it at the office and sends the results; it is a matter of seconds. After work, he works out at the gym, monitored by his digital coach. He's very happy with the progress he has made.

Going back home late, the car stops at the only flower shop open late as identified through his smartphone. Lukas wishes to celebrate some good news he just received: his bank has approved the mortgage application for the new house he and his family would like to buy. Payment for the flowers is made easily and securely through his smartwatch.

The digitally assisted lifestyle that Lukas enjoys relies heavily on the applications and data stored in the cloud. Imagine if the cloud services used by Lukas were not protected…

IMAGINE A BAD DAY IN 2020 FOR LUKAS

Lukas' smartphone is hacked by a competitor who does not want him to be on time for his important customer meeting, so he wakes up late. Neighbours manage to access his home network and play a bad joke on him: they invert the light, which turns off when he enters a room. He cannot get a cup of coffee as the automatic renewal was tampered with by a hacker who exploited another flaw in his network for fun.

During the customer meeting at work Lukas learns that the main competitor of his company will probably win the deal because the competitor managed to access the price list stored in the Corporate Cloud.

His insurance company gets his glucose rate by impersonating his doctor. Since the results are out of the medically accepted range, they decide to increase his insurance rate. His bank is also being notified of his health problem and, on this basis, decides to refuse the loan for the new house. On top of this, his bank informs him that his payment credentials have been misappropriated leaving his bank account empty. Nothing to celebrate on this day!

Back home, he discovers that his kids are not sleeping as he was told by the home monitor; they hacked it as he only used a simple password and went out to a party.

Trust is a must. Without security, convenient services bring more nuisance and disruption than benefits.

WHICH DIGITAL IDENTITIES WILL YOU HAVE IN THE HYPERCONNECTED WORLD OF 2020?

OUTLOOK

In 2020, travellers worldwide will mostly own electronic passports. In the European Union (EU), more than 250 million eID-cards will be held by its citizens, along with about 20 million eResidence permits held by third country nationals. More than ten EU member states will use eDriving Licenses, which can be used as a "pseudo-eID" document. In all regions of the world secure and convenient access to electronic government services will be possible via eID documents.

> ***In 2020, most state-issued identity documents will include an electronic identity secured by a chip***

This will both improve the quality of public services and make them more accessible to every citizen. At the same time, costs and fraud will be reduced due to the improved security of smart devices. In 2020, automatic border control and in-country control of identity will bring both convenience and security for the growing numbers of people crossing borders and also travelling within a country. This has been a major driver for the use of card technology in the new generation of electronic passports and national ID cards.

However, in 2020 eIdentification in a connected world will mostly be about convenience in everyday life, not about border control. In the public sector, citizens will be able to use state issued eIDs to access online public services. The private sector will have solved the fraud problems caused by weak identification and passwords thanks to smart, strong authentication solutions that are easy to use, secure and private.

WHAT CONSTITUTES AN "IDENTITY" IN A CONNECTED WORLD?

In the physical world, an individual's identity is unique and unmistakable and can be verified face-to-face. Individuals have a unique, clearly assigned identity.

In a connected world, a person can have multiple digital identities. On the one hand, a digital identity can be a self-declaration of personal data in accordance or not with the factual reality, e.g. name, age or any kind of civil status. On the other hand, a digital identity with the highest possible assurance level is issued only after face-to-face registration by a certified identity provider and protected by encryption and secure elements. A digital identity can therefore be genuine, provided by its real owner, or it can be fake or stolen and used for criminal purpose.

Low assurance level authentication of digital identities created by a username and password represent a very high risk of fraud. In fact, with enough information, anyone can claim anyone else's identity. And too many weak digital identities and improperly regulated identity providers make trust based exchanges difficult.

In both the physical and virtual worlds, citizens without identity do not exist. Without trustworthy identification it is impossible, for example, to rent an apartment, let alone buy a place to live, or to obtain work or to apply for any help from the government.

The presentation of the identity (e.g. identification) is made by means of information (e.g. a birth certificate) or a device (e.g. a card) or a biometric sample. The identity may be authenticated, that is verified, by means of a second factor: Something the individual knows (e.g. a password or a PIN code), or owns (e.g. a card or stored certified information) or biometric data.

With the smartphone, biometrics will become a natural way of authentication. Fingerprint readers, voice and face recognition are all available on this platform and this will contribute to convenience whilst privacy and security is upheld. Wearable devices will take biometric authentication solutions even further.

WHAT ARE THE RISKS?

In 2020, many individuals will be connected 24 hours a day, 7 days a week, at work through their computers, at home and in their daily business by means of smartphones, connected home appliances, connected glasses and watches, connected cars and contactless devices. This will apply in particular to the young generation of "digital natives".

> ***Digital identity theft can result in both financial losses and damage to the reputation***

For regular citizens, being constantly identified on the web poses the risk of divulging too much information: instantaneous identification of locations and activities, work activity and performance, habits, interests and lifestyle, etc.

Any and every activity can be tracked and traced. Big data can be abused by individuals and organisations for online solicitation, at any time and any location (a form of spam) and to commit fraud. It can also be abused to create a financial profile of potential clients and to set prices accordingly, e.g. the higher your income, the less discount an eMerchant will offer you.

Digital identity theft can result in both financial losses and damage to the reputation. There are specific risks related to children and young adults being online, among others for example digital harassment.

Public and private service providers can suffer from financial damage as well as damage to their reputation once data has been compromised. They may also face legal issues related to data protection.

The European Court of Justice has already established the right to be

forgotten[1]. Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Therefore, common EU rules have been established to ensure that personal data are safeguarded by a high standard of protection everywhere in the EU. The proposed EU Data Protection Regulation[2] also foresees specific rules for the transfer of personal data outside the EU to ensure the best possible protection of data being exported.

WHAT IS THE SMART SECURITY INDUSTRY'S CONTRIBUTION?

Safeguarding the liberty, security and privacy rights of citizens, in the physical as well as in the virtual world, is a fundamental task of governments. The eIDAS Regulation[3] adopted in 2014 represents a crucial step forward because it allows the implementation of an interoperable and secure environment for electronic identification and trust services in Europe, in due respect of European data protection rules. In terms of secure electronic identification, the industry has made proposals that require the use of certified devices to ensure an environment of trust, in the framework of this legislation.

The technology of secure elements provides the required security and privacy protection mechanisms, and empowers citizens to retain the control over their data. It has been successfully deployed for passports and eID documents worldwide.

Solutions that combine secure elements for storing biometric data as well as the software to carry out match-on-card[4] recognition in the secure element increase both user convenience and the protection of privacy by eliminating the need for network connections and databases. These solutions reach well beyond government ID and passport applications, notably replacing the PIN entry as the main means to access smartphones and payment applications.

Secure elements are also at the core of billions of SIM cards and payment cards being used every day, and secure elements are being embedded in smartphones for mobile payments. Furthermore, in over 20 countries worldwide, involving over 30 Mobile Network Operators, SIM based mobile ID services, as an individual tool for protection, have brought together mobility, convenience and security.

RECOMMENDATIONS TO POLICY-MARKERS AND STAKEHOLDERS

Eurosmart recommends to:

- Take advantage of smart security solutions such as secure elements, Trusted Execution Environments[5] (TEE) and biometrics to provide trust anchors for digital identities
- Require the use of certified devices for electronic identification to ensure an environment of trust, in line with internationally accepted standards for certification methods, tools and procedures
- Promote smart, strong authentication solutions that are easy to use, secure and private:
  - Simple to understand and easy to use because it relies on something you already have
  - Secure because it is provided by accredited identity providers and your credentials are stored and managed in a secure way
  - Private because your personal data is physically under your sole control, protected by a tamper-proof secure element

1 Judgment of the Court (Grand Chamber) in C-131/12 Google Spain v AEPD and Mario Costeja Gonzalez

2 COM(2012) 11 final – Proposal for a Regulation on the protection of individuals with regard to he processing of personal data and on the free movement of such data

3 Regulation 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market

4 Match on Card is the concept of matching and storing fingerprints on a smart card

5 The Trusted Execution Environment is a secure area of the main processor of a smartphone or any connected device. It guarantees that code and data stored inside are protected with respect to confidentiality and integrity

HOW DO YOU MAKE A PAYMENT IN 2020?[6]

Communication channels are bidirectional: there is reciprocity between the ability of the customer to connect and the ability of the merchants and payment service providers to localise their customers and propose tailored products and services to them. Ultimately, in 2020, a payment will be much more than a financial transaction, it will become a rich value proposition, integrating a wider commercial and transactional context.

> ***"By 2020, more than 50% of transactions will be made by mobile devices (Visa Europe)***

Merchants will be in a central position to offer goods with tailored payment instruments, minimising risks of financial losses in case of fraud. The knowledge of customer consumption patterns and of their solvency will boost personalised services: a package of commercial offers, merchant preferred payment instruments, special credit conditions, all incentivised with loyalty programmes. Mobile wallets will be the great enabler for this business revolution.

By 2020, electronic money will play a larger role alongside cash. It is expected that more than 50% of transactions will be made by mobile devices, including mobile contactless payment. In the European Union the mobile buying population will rise to more than 79 million in 2017[7]. In the United States, the value of mobile payments is forecasted to reach $90B in 2017, up from the $13B spent in 2012[8].

Mobile transactions will make payment systems more effective and may contribute to reducing the grey

OUTLOOK

An electronic payment transaction is basically a special exchange of digital information that results in a transfer of funds between the payer and the payee. Because payment data are digital information, there are multiple consequences of the telecommunication revolution for present and future payments.

The channels for payment are multiplying, as are the personal devices for access to services offered through those channels. These personal devices, if properly secured, are a perfect repository for payment instruments. This unprecedented ability to pay opens the door for new payment service providers offering innovative ways to pay.

economy. Financial inclusion of the underbanked and unbanked population is one of the most favourable socio-economic impacts of mobile payments. Dramatically lowering the cost of holding an account and of making payments coupled with innovative credit-related services will constitute key factors for economic development.

WHAT ARE THE RISKS?

The risks and threats associated with all electronic payments are the insufficient protection of the integrity of payment data which can lead to massive fraud. Fraud will migrate towards those payment instruments and channels perceived as most vulnerable by attackers. As a concrete example, the United States accounted for 47% of the worldwide payment card fraud losses in 2012, while they generated only 24% of total volume[9]. That was before the start of the migration from unsecure magnetic stripe payment cards towards EMV[10] chip cards, which will greatly help reduce this level of fraud.

New patterns for financial crime may also arise from using virtual currencies. Future virtual currencies will have to be designed with cryptographic functionalities that will enable their easy verification by the acceptor and prevent their use for money laundering purposes.

The multiplicity of payment networks and their connectivity will make the identification of fraud and financial crime patterns more difficult. From the industry's perspective, a breach relating to one particular innovative payment method will inevitably damage the reputation of other payment related innovations.

WHAT IS THE SMART SECURITY INDUSTRY CONTRIBUTION?

The worldwide migration towards smart card technology for payments makes it impossible to forge cards using exposed card data. The following three conditions should ensure the positive effects of innovative payment means: 1) A high level of security for any payment device and payment channel; 2) The privacy of an individual regarding his payments is respected; 3) Countermeasures to avoid misuse of new payment means for criminal purposes are established, endorsed and their efficiency monitored.

The smart security industry provides safe innovation able to sustain these conditions. Secure element-based payment means allow:

- Securing personal data and transactions through technology ensuring the secure storage and execution for transactions, preventing attacks on personal credentials both at rest and in transit. Secure elements function like a vault for personal credentials and are certified according to the highest security criteria, thus being the best possible protection against hackers' efforts;
- Identification and authentication, using PIN codes, one-time password (OTP) codes, biometrics and payment credentials;
- Ensuring interoperability by promoting standards for secure payment solutions that are accepted worldwide;
- Ensuring mobility with mobile payment solutions based on secure elements embedded in connected devices.

In addition, the smart security industry has a unique understanding of the business needs and constraints of the different sectors that have to collaborate to make omni-channel payment a reality (banks, payment schemes, Mobile network operators and governments). Successful current and future payment means rely on the adoption of common payment processing standards. For that purpose, the smart security industry is a reputed and competent participant in all relevant official and industry-led standardisation committees.

RECOMMENDATIONS TO POLICY-MAKERS ANS STAKEHOLDERS

Future payment means will become increasingly mobile and will involve proximity payments as well as remote payments. Different payment schemes are associated with different risk and fraud management approaches, which is why Eurosmart believes that guidelines will have to be provided, as well as strong security requirements and security evaluation methodologies. This will guarantee, in future, the practical impossibility to install malware that may capture and transmit any stored confidential information, or intercept data during transactions

Faced with the urgent need to protect online payment transactions, we propose that solutions be evaluated against the following criteria:

- Enable the customer to verify that the merchant website is legitimate
- Enable strong customer authentication
- Enable secure transfer of payment data and protection of customer data in merchants' databases
- Enable the customer to obtain a proof of authorised transaction, including transaction data such as merchant, amount, date and time

From a European perspective, this is particularly relevant with respect to the adoption and implementation of the proposed second Payment Services Directive[11], and the associated security guidelines for payment services on which the European Banking Authority and the European Central Bank are jointly working.

6 This section is mainly the contribution of the Smart Payment Association. This trade body addresses the challenges of the evolving payment ecosystem, offering leadership and expert guidance to help its members and their financial institution customers realise the opportunities of smart, secure and personalised payment systems & services both now and for the future.
see http://www.smartpaymentassociation.com/

7 EU Mobile Commerce Forecast, 2012 To 2017, Forrester, July 2012

8 US Mobile Payments Will Reach $90 Billion By 2017, Forrester, January 2013

9 Nilson Report, August 2013

10 EMV stands for Europay, MasterCard and Visa, a global standard for inter-operation of integrated chip card capable point-of-sale terminals and ATMs,for authenticating credit and debit card transactions

11 Proposal for a Directive on payment services in the internal market - COM/2013/0547 final

SECURITY OF CONNECTED OBJECTS

OUTLOOK

These one billion objects connected to mobile carriers' cellular networks will each include a secure element in the format of a SIM card adapted to M2M constraints. If we include connected objects using other networks, estimates reach 50 billion objects to be connected by the year 2020. Wherever people are, at the office, travelling, shopping, they will be surrounded by connected objects.

> ***"Cellular Machine-to-Machine[12] (M2M) will account for almost one billion of the 10 billion total mobile connections expected by 2020 (GSMA)***

At home, electronic devices such as TVs, fridges, alarm systems and electricity meters will all be connected and remotely controlled. Cars will be connected to other cars and to a service centre, analysing critical information about engine maintenance, safety, and traffic. Doctors will monitor patients' wellness from their desk whilst patients are travelling, with the ability to anticipate any health issues and to contact the patients. Already today, connected objects are being widely deployed and entering into our daily lives. This is the next big revolution after the computer and the mobile phone. However, the smart security industry strongly believes that innovation should not be achieved at the expense of security and privacy.

WHAT ARE THE RISKS?

Connected objects are deployed in an ecosystem where hardware (a connected object) is transmitting data captured by sensors to a service provider through a network (mobile network, Bluetooth, Wi-Fi, PLC). Major data breaches are becoming a monthly, if not a weekly occurrence. These breaches of trust are a threat to future benefits from cloud services and, by extension, for connected objects.

In some applications, such as smart energy, security and privacy have started to be addressed through recommendations, regulations and proper infrastructure. Unfortunately, this is not yet the case for the majority of connected objects which have not been designed to protect data against security and privacy breaches. In fact, connected objects are even more vulnerable to security attacks because there is no human element of control in the data collection, transmission and monitoring. Furthermore, most of the connected objects remain unattended giving attackers plenty of time to operate.

In a series of articles, two Norwegian journalists revealed how failing computer security affects us at home, at work and in the public space. They have shown that thousands of connected objects were left completely open, without any protection, and as such freely accessible by anyone over the Internet[13].

As far as privacy is concerned, connected objects can give third parties access to citizens' personal data including their habits, way of life and health condition. Private life is at risk of becoming open and visible. In another worst case scenario, an unscrupulous insurance investigator could find the evidence they need in an insurance claim by accessing the health data that have been transmitted to a doctor.

12 Cellular M2M refers to connected objects that use mobile carriers' cellular networks for data communication

13 "Null CTRL" project, available online at http://www.dagbladet.no/nullctrl/

WHAT IS THE SMART SECURITY INDUSTRY CONTRIBUTION?

The smart security industry designs and implements secure elements which are embedded into connected objects as well as solutions and services to manage the lifecycle of these objects. A secure element is a tamper-proof microchip designed to securely protect the secret cryptographic keys that are needed to set up secure communications between devices. It enables strong authentication and will authorise access only to authorised parties. Software solutions alone cannot provide the necessary level of protection required by most connected objects.

The smart security industry works on establishing regulation and standardisation to ensure interoperability as a key driver to facilitate the deployment of connected objects. Regulation has started within the smart grid ecosystem; it has to be extended to other sensitive applications. Smart security technology in connected objects can prevent a hacker from breaking into a private or public network - the intruder will face the same challenge as trying to find the secret PIN code of a payment card. In the same way it will keep a dishonest person from getting hold of the personal data in a health monitoring bracelet.

RECOMMENDATIONS TO POLICY-MAKERS AND STAKEHOLDERS

By 2020, every human being will have to deal with dozens of smart objects. Security and privacy will be essential.

The smart security industry has the technologies and solutions to solve these challenges; but it is equally important that international and national authorities take initiatives to protect citizens and companies against increasing risks to security and privacy by encouraging certification and standardisation, and supporting the integration and use of secure elements.

Regulation has started within the smart grid ecosystem and protecting critical infrastructure is a high priority. Policy-makers must continue with other sensitive applications.
The smart security industry has more than 20 years' experience in creating solutions combining convenience, privacy and security. It can help authorities in finding the right balance and implementing the right security technologies to protect people and data.

CONCLUSION

OUTLOOK

The services that Lukas uses in the 2020 scenario will reside fully in the cloud. The same already holds true or will be the case for your social media content, personal photos, financial information, health insurance information etc. Cloud services are transforming how people, businesses, and governments communicate and engage. The economic impact is very large. It has also generated societal change by connecting individuals and communities, providing access to information and education, and promoting greater transparency.

> ***In 2020, an estimated 12 billion secure elements will be shipped worldwide***

Already today, major data breaches are becoming a monthly, if not a weekly occurrence. As illustrated by the bad day scenario, these breaches of trust are a threat to future benefits from cloud services. And while liabilities for financial fraud on credit cards are clearly defined, who is protecting personal data such as health records that will be stored in the cloud?

Trust is at the core of good relations, and trust starts with an assurance that the person or entity you deal with is indeed who they profess to be. In the digital world we can achieve this trust by securely storing the credentials used to prove our digital identities in a tamperproof secure element, physically under the sole control of the individual.

Just as importantly, your digital identity and authentication provider must have both the ability and the will to protect your privacy. This means that rules for minimal data disclosure must be applied and a business model must be implemented that is not based on making money on personal data unless explicit user consent is given (so called privacy by default).
For the last two decades, the smart security industry has deployed billions of standardised, interoperable secure elements, protecting consumers and citizens while giving them access to digital services. In SIM cards, payment cards and electronic government documents, personal data are efficiently protected by tamper-resistant solutions including secure hardware, secure software and personalisation by the issuer.

For instance, payment card fraud has decreased to 0.036% thanks to the migration to the EMV standard. This demonstrates the efficiency of the security features developed by the smart security industry. In 2020, cloud services will not only be easy to use, but also secure and private thanks to smart, strong authentication, reducing the fraud threat of username/passwords:

- Easy to use and simple to understand because it relies on something you already have
- Secure because it is provided by trusted identity providers and your credentials are stored and managed in a secure way
- Private because your personal data is physically under your own sole control, protected by a tamper-proof secure element in the hardware

It is essential to draw citizens', companies' and policy-makers' attention to digital security challenges. Only internationally recognised standards and regulations can mandate the use of the highest means of security to protect personal data such as payment information, health data and biometric data.

Smart security solutions enhance the usability of digital services, while at the same time protecting privacy and combating fraud. Security necessarily comes at a cost, but fostering trust and avoiding fraud has an excellent return on investment.

EUROSMART
The Voice of the Smart Security Industry

ABOUT EUROSMART

Eurosmart is an international non-profit association located in Brussels and representing the smart security industry for multisector applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, developing Smart Security standards and continuously improving the quality of security applications.

Members are manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators, application developers and issuers who work in dedicated committees (security, electronic identity, mobile trust, marketing, communication). Members are largely involved in research and development projects at the European and international levels.

Eurosmart members are companies (Athena Smartcard, EM Microelectronic, FNMT-RCM, Gemalto, Giesecke & Devrient, Imprimerie Nationale, Infineon Technologies, Inside Secure, LFoundry, Linxens, Microsoft Corporation, Morpho, Nedcard, NXP Semiconductors, Oberthur Technologies, Samsung, STMicroelectronics, Toshiba), payment systems (Mastercard), laboratories (CEALETI), research organisations (Fraunhofer AISEC), associations (Smart Payment Association, Mobismart, Danish Biometrics) and independent experts (Michel Koenig, Jonas Andersson).

Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry".

For more information, please visit www.eurosmart.com

CONTACT

Oyvind Rastad
Eurosmart President
Rue du Luxembourg 19-21
B-1000 Brussels
Belgium

eurosmart@eurosmart.com

Tel: + 32 2 506 88 38
Fax: + 32 2 506 88 25