



Research Agenda



Veilig verbonden

ICT Innovation Platform
Security and Privacy





The Bloemenbeek Triptych
painted by the authors of the agenda
February 1st 2007, De Lutte, Twente



Authors and supporters

The agenda has been written by:

Author	Affiliation
Jan Piet Barthel	ictregie.nl
Dick Brandt	tntpost.nl
Philip Brey	utwente.nl
Jaap Halfweg	kpn.com
Pieter Hartel	utwente.nl
Gerard van der Hoorn	nictiz.nl
Bart Jacobs	ru.nl
Paul de Jager	tno.nl
Willem Jonker	philips.com
Bert-Jaap Koops	uvt.nl
Nanne Onland	dartagnan-biometrics.com
Michael Samson	nvb.nl
Jan Wester	minez.nl

The agenda is supported by:

Supporter	Affiliation
Asker Bazen	uniqkey.com
Arie van Bellen	ecp.nl
Bert Bos	chess.nl
Fred Eisner	abm.nl
Rik Janssen	stw.nl
Karst Koymans	uva.nl
Inald Lagendijk	tudelft.nl
Dick Leegwater	vka.nl
Sjouke Mauw	uni.lu
Wim Mooij	irdeto.com
Kees Nieuwenhuis	thalesgroup.com
Wim Hafkamp	rabobank.nl
Aernoudt Schmidt	leidenuniv.nl
Alwin Sixma	consumentenbond.nl
Robert Stegwee	capgemini.com
Henk van Tilborg	tue.nl
Tony van der Togt	minvenw.nl
John de Waal	ti-wmc.nl
Pieter Wagenaar	vu.nl
Nico Westpalm van Hoorn	portofrotterdam.nl
Marc Witteman	riscure.com



Preface

ICT empowers individuals through communication (GSM, e-mail, chat, blogs), fosters creative expression (YouTube, Wikipedia), and helps people to realise their economic potential (web shops). ICT optimises business processes so that value chains can operate in an efficient and targeted manner. As a result of these ICT-induced developments, our society is now largely dependent on the proper functioning of ICT. Security and privacy technologies play a pivotal role, because we will only be able to devote all our energy to promoting prosperity if we feel safe and secure, and if we have confidence in the ICT systems with which we are working.

The “Veilig Verbonden” research agenda sets out the challenges that must be met for ICT to continue to play its pivotal role in the years to come. The challenges have been selected as a careful balance between the desires, requirements and interests of the various stakeholders in seven key economic sectors for the Netherlands.

The “Veilig Verbonden” research agenda has been drafted by a group of domain experts from key industry sectors and government, as well as members of the Dutch academic security research community. The authors of the agenda form the nucleus of the ICT Innovation Platform Security and Privacy, an open interest group which operates under the auspices of the ICTRegie, the ICT Research and Innovation Authority of the Netherlands.

This research agenda is the first version, of a living document. Starting from the current survey of the most pressing research problems, the document will evolve into a full-fledged research agenda in the near future. New versions will be made available on our own (interactive) team site, which can be reached via the IIP portal on the ICTdelta website www.ictdelta.nu.

January 2008 (second edition),

Willem Jonker

Pieter Hartel

Paul de Jager (editors)



Vision

The vision expressed in this agenda is that a multi-disciplinary development, deployment and exploitation of ICT security and privacy know-how is crucial to promote continuity and innovation in the economic sectors and in Dutch society in general, and to ensure that the Netherlands is a reliable and innovative global business partner. In the digital world, ICT security is the key enabler of continuity for both the public and the private sectors because it ensures the proper and uninterrupted functioning of the underlying ICT infrastructures. Privacy gives individuals dignity and promotes individuality and autonomy. These are primarily important social values. However, individuals who feel free and secure are also encouraged to be creative and to exploit new opportunities, thus fuelling the economy.

Motivation

The Netherlands boasts the highest broadband penetration in the world. This versatile ICT infrastructure is currently being used to create a vital backbone infrastructure for all kinds of services, such as strong digital identities, an electronic health record and a nationwide smartcard-based public transport ticketing system for 16 million inhabitants. Government, business and individuals rely on the backbone infrastructure to support increasingly sophisticated business value chains, where trust and privacy are key elements. Thus, a digital world is being created which is affecting an increasing part of people's personal and professional lives. In order to realise fully this digital world we require three key success factors, all of which are readily available in the Netherlands.

Firstly, the Netherlands is a trading nation with a long-standing tradition of forging relationships of trust on a global scale. Secondly, the Dutch are individualists who value their personal freedom and privacy very highly. Thirdly, the Netherlands has a renowned security research community and a strong and innovative industry for applying and developing security technology. The Netherlands is, therefore, in a good position to expand the backbone infrastructure with the tools that are needed for successful business in the digital world.

Approach

In many current systems security is provided only as an add-on (the most prominent example is the Internet, which is based on the end-to-end argument). In some cases privacy is not given sufficient consideration (the issue of social security numbers is the main cause of ID fraud in the US). We believe that an appropriate level of security and privacy can only be provided by systems that have been designed to take into account security and privacy concerns right from the start. The platform will therefore actively promote an approach whereby security and privacy are treated as first-class citizens in any design activity, just like functionality, usability, performance, etc.



Introduction

To exploit the excellent starting position of the Netherlands and to mobilise and guide the security community, this document sets out a research and innovation agenda to address the security and privacy challenges in the digital world. This agenda provides concrete objectives that can be realised within the next 10 years. The objectives are tailored to key areas of economic and social activity in the Netherlands. The agenda is a joint effort and enjoys support from a wide range of stakeholders from industry, academia, government, and societal organisations. The agenda attributes importance to social, legal, economic and technical developments.

Security, privacy, trust and confidence

By *security* we mean confidentiality, integrity and authenticity. By *privacy* we mean data minimisation and user control. *Trust* is a relationship between people, whereby the trustee is expected to act in the best interests of the trustor. A person has *confidence* in a system when they believe that the system does what it is supposed to do.

Seven application areas

Talking about security and privacy makes most sense in a particular application domain. For example, privacy is not an issue for sea containers fitted with RFID tags, but it is for clothes fitted with RFID tags. In the agenda we identify seven application areas where security and privacy are important, based on the following criteria:

- ◆◆ The area is considered crucial for the Dutch economy and has a high potential for further economic growth.
- ◆◆ Significant innovation has already taken place and many opportunities for further innovation exist.
- ◆◆ The prospects of exporting technologies are good.
- ◆◆ Security and privacy are a prerequisite for successful innovation.

Objectives

The main challenges emerging from each area are identified and translated into a number of what we believe to be achievable objectives.

For each objective we indicate the priority, ranging from high (two diamonds ◆◆) to low (no diamonds).

The challenges and objectives from a number of areas overlap to some extent. This overlap is analysed at the end of this document.



Processes in the health sector are increasingly being supported by ICT, but ICT is also the key enabler of new methods of providing care, as exemplified by ambient assisted living. However, patient data is often spread across many care providers, such as the general practitioner (doctor), dentist, consultant (specialist), physiotherapist, hospital, pharmacy and, of course, the patient. Care providers must be able to access relevant information that is created and maintained by colleagues (such as medication records). Patients expect the same level of care whether they are at home, travelling or abroad. To a certain extent, the law gives patients control over who can access patient data so as to safeguard the *privacy* of the patient. The *security* of patient data is essential to ensure that doctors obtain the correct information at the right time. The retention period for patient data is long (up to 70 years) and this poses a significant challenge for the technical infrastructure that supports the healthcare system.

Stakeholders

The ministries of Health, Welfare and Sport (VWS), Interior and Kingdom Relations (BZK), Economic Affairs (EZ), patient associations, associations of care providers, insurance companies, and NICTIZ.

Economic relevance

In the Netherlands, an annual 300 million euros is spent to rectify incorrect treatment and medication as a result of healthcare professionals being unable to obtain accurate and complete patient data.

State of the art

The Dutch electronic health record (EPD) represents the state of the art. The EPD is a government-controlled system which uses a centralised pointer database to link patient data held by care providers. Patients and care providers are identified by unique identifiers issued by the government. Care providers use smartcards and PIN codes based on two-factor identification and authorisation. (Read only) access for patients to their own data is also controlled using two-factor authentication, using the SMS service instead of smartcards. Furthermore, Electronic Health Records are also being developed elsewhere.

Challenge

The main challenge in the healthcare domain is how to give authorised health professionals immediate and full access to all relevant patient data, subject to informed consent being given by the patient.



Aim and objectives

The aim is not only to realise the potential of the EPD system outlined above, but also to progress beyond the state of the art by fulfilling the following objectives:

- 1 Investigate how secure the current centralised architecture is compared with a distributed architecture.
- 2 ♦ Allow patients to manage their own electronic health records.
- 3 ♦ Study the effect of an EPD on the relationship of trust between patient and doctor.
- 4 ♦ Develop efficient and effective methods for standardisation and certification of the systems and interfaces used by care providers.
- 5 Provide care to a patient who opts out of the EPD (which he has a legal right to do).
- 6 Ensure that patient data is available under special circumstances, e.g. to doctors abroad, doctors making house calls, doctors standing in for a colleague, in circumstances when there is a power failure, etc.
- 7 Develop business incentives for an individual care provider to invest in an EPD-compatible system.
- 8 Be able to privatise (parts of) the service.
- 9 Prevent inconsistencies in the many databases involved.
- 10 Cope with the many legacy systems at doctors' surgeries, hospitals, etc.
- 11 ♦♦ Support new methods of extra-mural and ambulant care with secure and dependable ICT.



Internet and telecom

Telecommunications and the Internet are merging to become more and more an All-IP environment, where traditional telephony (voice), television (video) and data exchange are integrated into a multi-channel system. Services can be provided to large groups of users (broadcasting and information sharing), specific groups (narrowcasting and user communities) as well as single users. From the consumer perspective this new world is seen as the source of all information, an opportunity to socialize and a way to communicate. Consumers clearly express the need to contribute actively as a content provider (wikipedia/Youtube). The service providers, however, are expected to initiate innovations, manage issues such as cyber crime, and ensure consumer privacy and the availability of the services.

Stakeholders

ISPs (such as XS4ALL), network providers (such as KPN), service providers (such as Tele2), content providers (such as OD2), and the ministry of Economic Affairs (EZ).

Economic relevance

Consumers have a limited knowledge of security and privacy technology; they simply expect the providers to take care of these issues. The need for a secure and dependable All-IP environment is a prerequisite for the success and usability of the Internet in its vital role within the society of the future.

State of the art

In the traditional (PSTN, PABX, ISDN) telecom domain the telephone number is used to provide a unique end-user identification, which can often be linked to the identity of a person or location. In the Internet this is not the case, and this has led to the development of a large variety of incompatible identity management systems. This increased complexity has a detrimental effect on the end user's confidence in the services offered. The data-retention regulations raise privacy concerns that need to be addressed as a matter of urgency.

Challenge

The main challenge in the Internet, and increasingly in the telecom domain, is to give end users confidence in the security and privacy of communication, and to make the security convenient and transparent. It is essential to establish a (global) legal environment to prevent cyber crime and create trust, although this legislation should not hamper innovation.

Aim and objectives

The aims are to provide mechanisms and procedures that allow end users to:

- ❖ choose either to maintain anonymity or to identify, authenticate and/or authorise (IAA) other end users in an efficient and effective manner, based on centralised or decentralised mechanisms.
- ❖ assess the security and privacy level of the services offered.

This leads to the following objectives:

- 1 Develop IAA standards for the end user in the technical, social and legal domains.
- 2 ♦ Provide a transparent framework of trust that supports reasoning about the security level provided.
- 3 Improve the level of user friendliness of IAA so that it is acceptable for the end user.
- 4 Foster confidence in IAA.
- 5 ♦ Manage chains of trust between operators and end users, in any combination.
- 6 ♦♦ Make IAA and frameworks of trust independent of the underlying infrastructure so they can cope with incompatible life cycles and innovations.
- 7 Agree and harmonise international legal and regulatory frameworks to promote trust and prevent, detect and bring prosecutions for cyber crime.
- 8 Create alternative ways of communication in social networks (e.g. SecondLife and MySpace).





Semi-public spaces

The continued operation of semi-public spaces such as airports, harbours, railway stations, as well as sports venues and concert halls is vital to economy and society. ICT is increasingly being used to facilitate, monitor and control the movements of people and goods in such areas.

Stakeholders

Amsterdam Airport Schiphol, Port of Rotterdam, Nederlandse Spoorwegen, Air France KLM, the Ministries of Transport, Public Works and Water Management (V&W), Justice and Defense (Justitie), KNVB, NEDAP, Dartagnan, TNO, TNT.

Economic relevance

The interests are considerable; The Port of Rotterdam and Amsterdam Airport Schiphol together account for approximately 12% of GNP in the Netherlands (source: Ministry of Economic Affairs). Furthermore, millions of people visit sports venues and concerts every year.

State of the art

Without consent. Camera surveillance is a common way of monitoring public spaces. The trend today is towards systems that can automatically detect anomalous behaviour. Many systems are a threat to privacy, a problem which is compounded by the high degree of false positives that are characteristic of state-of-the-art systems. A major technical breakthrough is needed to advance the state of the art in this area sufficiently.

With consent. In situations where access control is used to control flows of people (e.g. security & border control, stadium access) there is a visible trend towards utilisation of biometric identifiers and automated recognition technologies (e.g. radio frequency technologies) to identify the flow of people and goods. There is a proven need for further development of technologies that can positively and negatively identify and recognise flows of people and goods throughout logistical processes without having a negative impact.

Challenge

The main challenge is to protect the primary processes by monitoring people unobtrusively when they are going about their private business.



Aim and objectives

The main aim is to be able to optimise the logistical primary processes. This gives rise to the following objectives for access control in semi-public spaces:

- 1 ♦ Achieve standardisation and certification of processes and systems.
- 2 Avoid centralised (single point of failure) approaches.
- 3 ♦♦ Balance civil rights against the need for monitoring, controlling and profiling.
- 4 Balance the effectiveness and efficiency of monitoring approaches.
- 5 ♦ Synchronise technical developments with the evolution of the legal and regulatory frameworks, as well as social developments.
- 6 Deal effectively with insider attacks.
- 7 Manage value chains in which, for instance, foreign governments play an important role.
- 8 ♦ Consider proportionality (for example, is it ethical to use RFID implants for employees?)
- 9 Improve the user friendliness and accuracy of biometric technologies.
- 10 Comply with international legal and regulatory frameworks, official and de-facto standards.



Finance and insurance

Financial institutions such as banks and insurance companies are keen to increase the level of convenience for their customers and to save costs by moving as many services as possible from bricks to clicks. The Internet offers significant potential for greater integration in the value chain, with security as one of the major enablers. However, increased automation in the value chain reduces the amount of direct contact between the customer and his bank. The Internet should offer possibilities for increasing this direct contact again (when required), with sufficient guarantees for authentication and confidentiality.

Stakeholders

Banks, insurance companies, government, security brokers, ICT companies, customers (from retail customers to the large corporations and public organisations), supervisors, standardisation bodies, etc.

Economic relevance

The current level of investment in security infrastructure is significant. The economic relevance for the banking community is the need to maintain customer confidence in the current products and providers so that the usage of the e-products will increase further. New opportunities are being sought to cut back yet more manual actions. The financial sector is a crucial part of the economy. In the Netherlands, almost everyone (older than approximately 15 years) and all organisations have at least one active bank account. About 4 billion payment transactions are processed each year. The balance total of the Dutch banks exceeds 3×10^{12} euros.

State of the art

The Dutch banking community uses the Internet extensively for standard customer transactions. For example, the holders of over 6 million bank accounts have an Internet contract, so that it is possible to make transactions (payments and / or securities), open a new account, and even negotiate a mortgage via the Internet. Customers are confident that the Internet banking solution in the Netherlands is sufficiently secure. This confidence made it possible for Internet banking to grow rapidly and it is likely to boost growth further. Most Dutch high-street banks and banks in a number of other European countries use two-factor authentication for transactions; banks that lag behind in this respect are more vulnerable to fraud, (e.g. phishing attacks). Customers currently using Internet banking are strongly advised to maintain the security of their systems (e.g. by installing a fire wall, virus scanner, anti malware, and by checking that they use a secure website), but this is not convenient.

Challenge

The main challenge is how to offer services remotely while still maintaining the high security standards of the banks and the customers' high level of trust in the banking community.



Aim and objectives

The main aim is to use new communication media (Internet, mobiles, TV) for providing services. This gives rise to the following objectives:

- 1 ♦ Make the Internet more secure for financial transactions, which will lead to greater convenience for end users when it comes to maintaining the security of their systems.
- 2 Increase the platform independence of the services and their security provisions.
- 3 ♦ Investigate alternative, distributed trust models (Boober.nl, Hawala).
- 4 Increase flexibility, for example card-less ATM usage, or electronic purse recharge at home.
- 5 Create new payment models, including anonymous payments, payments effectuated via mobile operators, and micro payments.
- 6 Leverage the trust that end users have in banks to the digital world.
- 7 ♦ ♦ Find effective ways to combat financial cyber crime, including financial identity fraud and phishing.
- 8 Create new authentication methods, using mobile phones or other contactless devices.



Transport and logistics

In transport and logistics the partners in a value chain manage three streams. The first stream consists of goods and people collected, stored temporarily (or held in transit), transported and delivered. The second stream consists of financial compensation for the logistics and transport services rendered. This stream flows in the opposite direction. The third stream consists of information, which flows in both directions. The trend is to move from replenishment to direct delivery, thus avoiding expensive intermediate storage in the chain. The margins are generally very low, and transport and logistics is a buyers market.

Hence cost reduction is essential.

Stakeholders

Parcel, express and postal companies, Port of Rotterdam, Transport en Logistiek Nederland (TLN), the Ministries of Economic Affairs (EZ), and Health, Welfare and Sport (VWS), retail outlets, public transport companies, users of the roads and railways.

Economic relevance

The Port of Rotterdam processes 10 million cargo containers per annum.

State of the art

Transport and logistics is responsible for about 10% of the GNP of the Netherlands.

All partners in the value chain are able to track and trace goods from collection to delivery. The value of the goods determines to a large extent the issues and the sophistication of the technology. For example, a growing number of cargo containers are equipped with GPS equipment and tamper-evident locks. The OV chipkaart (electronic ticket for public transport) represents the largest roll-out of an e-ticketing system in the world. Plans for an advanced road pricing system are being reconsidered with a view to easing road congestion. RFID tags are too expensive for many applications; hence the search for less expensive technologies has a high priority.

Challenge

The main challenge in the domain is to ensure business continuity while making the value chains as short and responsive as possible. A shorter chain has fewer participants and thus lower cost. A responsive chain delivers goods and payments faster, again lowering costs. However in a shorter chain the risks of interruption of the logistics and transport services will increase and thus business continuity risks will increase.

Aim and objectives

The main aim is to ensure the integrity and availability of the goods, information and compensation streams. This gives rise to the following objectives:

- 1 Develop methods and tools to balance redundancy needed to obtain robust streams against the consolidation of value chain partners needed to achieve short and responsive chains.
- 2 ♦ Develop risk management methods that take the dependencies between the streams into account.
3. Develop advanced identity management methods to link the movement of objects in the three streams.
- 4 ♦♦ Introduce natural tag technology into the very low-margin market of goods transportation, with a keen eye on the privacy issues.
- 5 ♦ Research the security and privacy aspects of road pricing and transport-surveillance systems.
- 6 Confirm to international regulations, such as the Container Security Initiative launched by the US department of Homeland Security in 2002.
- 7 ♦ Develop supply chain oriented business continuity plans.





The government has identified three “arenas” where security is paramount. The first is critical infrastructures, where the government has to ensure continuity even though many of the critical infrastructures are operated by the private sector. The second arena is cyber crime, which includes everything in the digital world that threatens the life of the citizen directly, such as malware, spam, identity fraud, etc. The third arena is policing and prosecution, where special skills are required that have not been taught to a significant percentage of the current workforce.

In many cases the government has different roles where security is involved. On the one hand, it provides services (such as the tax service, issuing passports, granting subsidies) and, on the other, the government is itself an end user (such as the telephone service, and the Internet). The government thus depends on the private sector to provide part of the security services it needs. However, the government is also responsible for the security and protection of the privacy of citizens.

Stakeholders

Banks, Diginotar, Interpay, central government, local government, semi-government organisations as well as the healthcare, traffic and education sectors.

Economic relevance

The government is responsible for the management of electronic identities. These identities are necessary for all kinds of commercial and official transactions. The government is thus also responsible for creating and fostering confidence in the systems that are being implemented. The government has to face up to any liability for damage that may be caused by the corruption of these identities. This damage includes financial, health and image risks and could assume enormous proportions. On the other hand, private businesses might not develop because they depend on these mandatory public identities but do not have access to them. Here lies a potential productivity loss.

State of the art

The main objective of the government is to improve the accessibility of its services for citizens and for businesses.

To achieve this objective the government is implementing:

- ❖ the DigiD, a large-scale digital authentication infrastructure and identity management service.
- ❖ the e-NIK, which provides the holder with digital signature capabilities.
- ❖ the e-passport, a biometric electronic national identity card.

Future developments may also include e-voting.

Challenge

The challenge for the government is to perform the role of both service provider and end user within a complex multi-actor environment, finding a balance between civil rights and public interests, such as security, and between the rights and desires of the citizen on the one hand and the needs of industry on the other hand.



Aim and objectives

The aim is not only to realise the potential of systems such as the DigiID and e-NIK, but also to progress beyond the state of the art by meeting the following objectives:

- 1 ♦ Foster inter-sectoral use of the unified identity management services, such that the system remains manageable and applicable.
- 2 Arrange and attribute responsibilities appropriately, transparently and fairly in value chains.
- 3 Support policing and prosecution, particularly to combat ID fraud.
- 4 ♦♦ Safeguard the privacy of the citizen, particularly by promoting identity-poor, attribute-based services.
- 5 ♦ Create new ways of promoting democracy, for example through e-voting.
- 6 ♦ Deploy remotely services that currently require physical presence.



Creative Industry

Content plays an important role in education, training and entertainment. The traditional producers of content are the record, film and gaming industry, as well as publishers. However, individual artists and consumers are increasingly interested in producing and distributing their own content (YouTube, Flickr, Skoeps). All aspects of copyright are a universal concern.

Stakeholders

International and national producers and distributors of music and video content, games, content-sharing applications and sites on the Internet, European and national legislators, industry (especially in its role as a contributor and adopter of standards), consumer organisations.

Economic relevance

The creation and distribution of content is an increasingly important part of our economy that makes extensive use of Internet technologies to reduce the cost of distribution. The content industry will thrive only if the producers of content are compensated in a fair way. We are on the verge of a new revolution where anybody can participate and become a small or large content producer. Gaming has its own security challenges. In large on-line games (such as World of Warcraft, with 8 million players and an annual revenue of over 1 billion dollars) it is crucial that game play is fair.

State of the art

All systems currently fielded to protect intellectual property have been broken. Incompatibility problems often mean that content protection systems prevent consumers from enjoying the content they have just bought. Individual end users have little scope for controlling the use and distribution of the content to which they contribute and which they make available on the Internet.

Challenge

The challenge is to make it easy and convenient for content producers and consumers to respect each other's rights and interests, in all types of content creation and enjoyment.

Aim and objectives

The aim is to be able to produce, distribute and enjoy digital versions of content efficiently, whilst offering effective compensation for producers of creative content. This leads to the following objectives:

- 1 Develop methods for creating, tracking and tracing content (for example, using watermarking). These methods enhance more strict forms of content protection, like encryption.
- 2 ♦ Research and harmonise the relevant legal and regulatory frameworks.
- 3 Improve interoperability of content protection methods through standardisation.
- 4 Facilitate the use and exchange of content across modalities (PC, mobile phone, consumer electronics).
- 5 Respect content provider rights and at the same time comply with content-usage patterns that consumers consider normal.
- 6 ♦♦ Offer easy-to-use methods and tools that would allow consumers to become fully-fledged producers of content, including mechanisms for compensation.
- 7 Develop new versatile carriers with enhanced copy-protection facilities.
- 8 ♦ Research new ways of enforcing copyright and protecting consumer rights and privacy.
- 9 ♦ Research emerging alternatives to copyright, such as the Creative Commons, open-source licenses and the copyleft movement.
- 10 Align the world of online games with the real world in terms of privacy and accountability.





Research topics

In the description of each of the seven application areas above we often mention the same or similar research topics. Although in the long term there will hopefully be generic solutions that will apply to many of the application areas, within the framework of this agenda the practical, legal, social and economic issues in each of the application domains are so different that the research topics are best studied in those application settings. In the list below we indicate some of the specific implications of each of the seven application areas for the seven most important research topics:

a. Identity management.

Each application area governs an important aspect of the digital life of the citizen, so the digital identity of people is a key element of study. However, in some areas (health, governance) a single authority is responsible for issuing credentials that certify the identity and qualifications or attributes of people. In some areas (telephone, post) a union of service providers is responsible for issuing unique identities (telephone numbers, street addresses). In other areas there is no single authority (and there is unlikely to ever be one) which will control identities. Therefore, different identity management solutions are needed to cater for these various needs.

b. Data and policy management.

In the application areas a variety of data plays a key role. However, the confidentiality, availability, authenticity and integrity requirements for different kinds of data can vary greatly, both in the technical as well as in the legal sense. For example, health records must be kept for 70 years, and therefore require strong security, whereas other data is almost ephemeral, such as the data kept by RFID tags.

c. Infrastructure.

The focus of security research for the infrastructure lies in areas such as software security, secure kernels and smartcards.

d. Economics and Risk management.

Some application areas are high volume low margin (transport and logistics, Internet and telecom), whereas others are high margin low volume (health, access control in semi-public spaces). Security and privacy solutions that are applicable in one area may therefore be totally unsuitable in another. Risk management is one of the main tools for assessing the economic impact of security and privacy.

e. Regulation and ethics.

Each application area is a multi-actor system, where large and complex value chains are in operation, involving public and private partners that have to work together to provide attractive services. However, the various application areas fit in different regulatory frameworks, and privacy expectations may differ. For some application areas the regulatory framework can be implemented at national level to a significant extent, but for other areas the regulatory framework is dependent on the EU and on international regulatory instruments. Awareness programs, codes of conduct and guidelines are key to improving the transparency of the technology and to offering users a real choice.

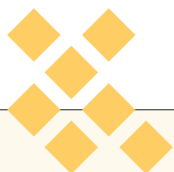
f. Certification and International Standardisation.

Value chains cannot operate unless mechanisms and processes are standardised and certified. Security and privacy will have to match the standards in the different application domains. Examples of relevant standardisation efforts in which the IIP is involved include the liberty alliance for identity management and the continua consortium for healthcare. Other relevant standardisation efforts are undertaken by ISO, the IEEE, IETF, ENISA, etc.

g. Methods and Tools.

Security engineering is a relatively new field and therefore lacks the maturity required to design, build and test cost-effective secure systems. As a result, security is often implemented as an add-on, instead of being designed into the system right from the start. While considerable progress has been made in specific areas, such as security protocol analysis, a sound engineering method for security is still a long way off.

In addition to these seven specific research topics, we consider it important to encourage grass roots initiatives and to provide ample room for blue skies and fundamental research.



The research agenda at a glance

The table below provides a mapping of the seven research topics onto the seven application areas, listing the main research issues in the intersection of the research topics and the application areas. For example, in the bottom right-hand corner “Watermarking” is mentioned as the main issue for security and privacy research into methods and tools in the creative industry. Watermarking is a promising method for tracking and tracing content, but a significant amount of work has yet to be done to make it effective and efficient. There are many other issues that deserve attention, but Watermarking is considered to be most important. Similar considerations apply to the other 48 entries in the table. It is difficult to do justice to the nature of each of the research issues in a single word. However, we believe that the mapping provides a useful summary of the most important issues, highlighting the major differences between each of the research topics and each of the application areas.

Main Issue	1. Healthcare	2. Telecom	3. Public Spaces	4. Finance	5. Transport	6. Government	7. Creative Industry
a. Identity management	Integrity	Identity portability	Multi purpose	ID theft	Availability	ID theft	ID theft
b. Data & Policy management	Integrity	Abuse	Privacy	Integrity		Integrity	Usage control
c. Infrastructure	Heterogeneity	Interoperability	Safety	Auditability	Traceability		Interoperability
d. Economics & Risk management	Prevention of errors	Multi-channel		Push back	Cost reduction	Accessibility	Electronic distribution
e. Regulation & ethics	Patient in control	Privacy	Privacy	Fraud	Fraud	Deregulation	Copyright
f. Certification & Standardisation	NEN7510 Hipaa	ISO		Basel II		Common criteria	Licensing authorities
g. Methods & Tools	Software	Protocols	Biometrics	Analysis	Lightweight crypto	Secret sharing	Watermarking

The table below shows how the research topics correspond to the four long-term challenges identified for the theme ‘Digitale Veiligheid’ in the NOAG-ict (de Nationale Onderzoeks Agenda ICT 2005-2010):

NOAG-ict theme ‘digitale veiligheid’ long-term	IIP Veilig Verbonden Research topics		
1: secure information management	a. Identity management	b. Data & policy management	
2: how to foster trust and confidence	c. Infrastructure	d. Economics & risk management	e. Regulation & ethics
3: integral certification	f. Certification & standardisation		
4: secure systems engineering	g. Methods & tools		

In its 7th framework programme, the European Commission has identified many relevant issues that we address in this agenda, such as trusted computing infrastructures, identity management and privacy enhancing tools, and security and confidence in dynamic and reconfigurable service architectures.



The ICT Innovation Platform

The owner of this research agenda is the ICT Innovation Platform (IIP), which comprises representatives of knowledge generation, knowledge transfer and knowledge exploitation, i.e. the entire knowledge chain in the field of security and privacy. A profile description of an IIP can be found in the memorandum: “framework of ICT Innovation Platforms”, from ICTRegie, the Netherlands ICT Research and Innovation Authority (07-NROI-065). IIPs were formed as a result of the actions formulated in the ICT-Innovatieagenda 2006-2010, which ICTRegie released in 2006. The concept of the European Technology Platforms has provided further inspiration for the creation of IIPs.

The ICT Innovation Platform

The mission expressed in this agenda is to foster security and privacy in the digital world. *Security* is one of the key factors to ensure that the primary processes can continue to function normally. *Privacy* is one of the key factors to ensure that creative initiatives of individuals are nurtured and promoted. Interoperability of technologies and processes is paramount, as everything in the digital (and the real world for that matter) takes place in a value chain, across sectors and across borders. What matters most in the digital world is how people, businesses and governments *work together*.

To sustain and improve ways in which we can work together in the digital world, the following objectives for security and privacy have been identified:

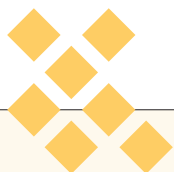
- 1 Make security in the digital life of the *citizen* transparent and make privacy something that can be taken for granted.
- 2 Improve the efficiency and effectiveness of doing *business* in a secure manner and with an appropriate degree of privacy.
- 3 Make it easy for the *partners* working together to agree on where the responsibilities for security and privacy in a value chain are allocated and/or shared.
- 4 Improve interoperability by means of standardisation and integration of security and privacy in the technological *infrastructure*.
- 5 Encourage dialogue between technical developments in the digital world and *legislation* and *regulation* on security and privacy.
- 6 Encourage *grass roots* initiatives such as Creative Commons, which have the potential to revolutionise the digital world.
- 7 Avoid social exclusion by improving the usability of technology.



Activities

The activities of the platform include:

- 1 Updating and maintaining the agenda.
- 2 Formulating specific challenges for security and privacy.
- 3 Performing a regular needs analysis and demand articulation.
- 4 Creating an action program, based on prioritisation of agenda items and roadmaps.
- 5 Seeking opportunities, together with and/or supported by ICTRegie, to ensure parts of the agenda and action program are implemented through research planning and programming.
- 6 Boosting public confidence in new security and privacy technologies and ensuring use thereof by involving consumer organisations, generating publicity, etc.
- 7 Providing advice to proposers of research projects.
- 8 Keeping a watchful eye on developments that will impact the agenda.
- 9 Encouraging the submission of research proposals.
- 10 Promoting standardisation efforts in the fields of ICT security and privacy.
- 11 Cooperating closely with the national programme 'Digibewust', through which the business community, government and NGOs are working towards a safer information society by raising awareness and setting up pilot projects and R&D programmes.



Knowledge management

The IIP aspires to promote the generation, transfer and exploitation of knowledge, involving academia, industry and government.

Knowledge Generation

Schools and universities will both extend the curricula in relevant disciplines and create new specialised security curricula, such as the Kerckhoffs master, to teach more students at undergraduate and PhD level the theory and practice of security and privacy. The content of the curricula will be influenced by long-term research issues put forward by market parties and civil society. This guarantees graduates that their knowledge and skills will match job opportunities. PhD students will form an integral part of the Dutch security research program to ensure that sufficient critical mass is created in the proper areas, such that society can benefit optimally from the results. Collaboration between different universities will be organised to pave the way for students to follow related security courses, to maintain a broad vision of security and privacy research in the Netherlands, and to work together on related, multidisciplinary security projects.

Joint research labs will facilitate experiments with the latest security tools and mechanisms and give students the practical experience that is needed for a complete security education. This national collaboration will enable trainees to find posts in the appropriate companies and/or research institutes.

Knowledge Transfer and Exploitation

The ambition of the agenda is to boost the process which transfers knowledge generated by academia and the research laboratories to society, industry and government, so that new practices, services and products can be developed more efficiently. The main approach is to ensure that all relevant market partners are already involved in the early stages of research and development so as to ensure that the research is highly relevant to the market partners and that the resulting knowledge can indeed be exploited effectively by these market parties.

Knowledge transfer will be organised in various ways, such as collaboration in R&D projects, consultancy, transfer of MSc and PhD students to industry, symposia, knowledge networks, etc.

In addition to knowledge transfer as a key enabler to exploitation, complete new economic activities will also be set up as a direct result of the research. The IIP will actively look for such opportunities and will support incubators, spin-offs and start-ups.

To optimize the possibilities of knowledge transfer and exploitation it is essential that research and industry partners work continuously on the further development and refinement of the Veilig Verbonden strategic research agenda.

The IIP is fully aware of the fact that IPR plays a key role in the transfer and exploitation of knowledge. Given that IPR arrangements are tailored to specific situations, the IIP does not provide an IPR framework but leaves this up to individual parties and projects.



Conclusions

The Netherlands forms an open society with a traditional economic basis in transport (of goods) and services. Its unique strength lies in the “polder-style” consensus models which favour integrated solutions to value chain-related problems. If we wish to safeguard our prosperity into the digital age we need to be a leading force in the development and building of appropriate models and infrastructures, making the most of the head start we already have in broadband and e-authentication, for instance. These new digital infrastructures need to be well balanced: on the one hand they must be open to provide ample scope for individual (social and economic) activities, autonomy and privacy; and on the other hand they need to be secure in the sense of being resilient and resistant to attack, so that vital social and economic activities can continue unhampered. To achieve such a balance we require models for security and privacy that follow closely local cultures (the way that people work and interact). They will form the basis for all other e-activities, ranging from healthcare and communications to finances and transport.

The IIP Veilig Verbonden will address security and privacy research challenges through an ambitious research agenda that addresses all strategic sectors of the Dutch economy. In each of these sectors the agenda will guide the necessary development of knowledge by fine-tuning the overall research in the fields of Identity management, Data & policy management, ICT Infrastructure, Economy of security and privacy, Regulation & ethics, Certification & standardisation, and Methods & tools to the needs of the specific sector. In addition, there will be room for blue skies and grass roots initiatives to foster innovation and economic growth.

The ultimate aim of the platform is to make a significant improvement, both in terms of the security of products and services and the privacy of users.



Research Agenda

ICTInnovationplatform
powered by **ICTRegie**