



#1

Area i: Security and Privacy in e-Government/e-Business

Title: Secure systems design and PKI

Explanation: What is the problem?

Current systems do not satisfy security requirements. Ways must be found to integrate issues such as OCSP, time stamping and trust lists in a secure system design.

Industry and government: Who are faced with the problem?

Government and private industries;
Enschede/SDU

Universities and knowledge institutes: Who can solve the problem?

Nijmegen: secure-systems engineering
TUD: System engineering
TUE and UT: protocol design

Further agreements: Who does what and when?

None

#2

Area i: Security and Privacy in e-Government/e-Business

Title: Role-based biometric authentication with PKI

Explanation: What is the problem?

- (1) The use of biometrics for authentication introduces a privacy problem: the user's biometric template can be stolen and illegally used, or information about the user's physical condition may be derived from it against his will.
- (2) For certain applications, the identity of a person is not required, but it merely has to be determined whether he or she is allowed to use the application.

Anonymous biometrics (generation of a PIN) directly from the biometric input needs to be studied as a solution.

Industry and government: Who are faced with the problem?

All sorts of access control (government, private, commercial);
Philips

Universities and knowledge institutes: Who can solve the problem?

CWI, UT

Further agreements: Who does what and when?

Contacts between Philips, CWI, UT exist.



#3

Area ii: Security and Privacy in Ambient Intelligence

Title: Biometric authentication for mobiles

Explanation: What is the problem?

Mobile devices (handhelds, PDA's) may require immediate and fast access without lengthy authentication protocols or even explicit user actions. (Transparent) biometric identification may solve the problem. Research questions include: which (combination) of biometrics, how to combine them, how to integrate in a networked security system?

Industry and government: Who are faced with the problem?

Philips, Telecom industry, Mobiles, PDA, public workers (police men, health care...)

Universities and knowledge institutes: Who can solve the problem?

Philips, UT, TUE

Further agreements: Who does what and when?

Contacts between Philips, UT and TUE exist.

#4

Area i: Security and Privacy in e-Government/e-Business

Title: Privacy of electronic IDs

Explanation: What is the problem?

A physical ID such as a passport must be handed over to an official for inspection. The original document is then returned to the holder, and the official cannot keep a copy of the document. The holder of an electronic ID on the other hand must assume that a perfect digital copy of her ID remains in the possession of the official. This fundamental difference between physical and electronic ID poses a significant privacy problem for the holders of electronic documents. How can this problem be solved?

Industry and government: Who are faced with the problem?

Any organisation issuing electronic IDs, including the ministry of foreign affairs, municipalities, companies, schools, universities;
Enschede/SDU

Universities and knowledge institutes: Who can solve the problem?

UTwente, CWI

Further agreements: Who does what and when?

No further agreements at this moment.



#5

Area i: Security and Privacy in e-Government/e-Business**Title: An architecture for personal management of privacy / owner-controlled privacy.****Explanation: What is the problem?**

Important points to be addressed:

- Definition of privacy,
- Personal data control (by compartmentalization, or by using licenses),
- PET for identification and legitimization,
- Privacy components and protocols.

Industry and government: Who are faced with the problem?

- System developers,
- Public and private sectors (government agencies, medical and financial institutions),
- Enschede-SDU.

Universities and knowledge institutes: Who can solve the problem?

VU, TUD, UT, TU/e, STW, Rand Europe, Telematica Instituut, TNO.

Further agreements: Who does what and when?

No further agreements at this moment.

#6

Area i: Security and Privacy in e-Government/e-Business**Title: Certificatie van Java smart card applicaties****Explanation: What is the problem?**

Op de nieuwste generatie van smart cards (chipkaarten) kunnen verschillende kleine computerprogramma's draaien, voor verschillende toepassingen. De programma's zijn geschreven in de bekende programmeertaal Java. Om voldoende vertrouwen in de veiligheid van dit soort kaarten te krijgen is het van groot belang dat deze Java programma's precies doen wat ze zouden moeten doen: het functionele gedrag moet precies geformuleerd en vervolgens vastgesteld worden, liefst door onafhankelijke partijen.

Industry and government: Who are faced with the problem?

De afdeling TNO-EIB in Delft <www.tpd.tno.nl/smartsite157.html> heeft een wereldwijde reputatie op het gebied van evaluatie van smart cards. Deze evaluaties betreffen vooral de hardware van de kaart. In toenemende mate vragen klanten echter om evaluaties van Java applicatieprogramma's.

Belangrijke klanten van TNO-EIB zijn de grote banken en credit card maatschappijen. Verder voert TNO binnen Nederland veel certificaties uit.

**Universities and knowledge institutes: Who can solve the problem?**

Binnen de Universiteit van Nijmegen heeft de groep Security of Systems <www.cs.kun.nl/ita/research/projects/loop/> jarenlange ervaring op het gebied van correctheid van Java programma's, vooral voor smart cards. Deze groep heeft de kennis, ervaring en tools in huis om op verschillende niveaus van zekerheid te komen tot certificatie van kleine Java programma's.

Further agreements: Who does what and when?

Een eerste overleg heeft plaatsgevonden op 10 maart 2003, waar besloten is om inderdaad te gaan samenwerken. Op basis van de gepresenteerde mogelijkheden vanuit Nijmegen zal TNO in overleg met haar klanten een nadere uitwerking geven van de gewenste certificatie technieken voor Java programma's. Deze technieken zullen zonodig verdere uitgewerkt en toegespitst worden in een gezamenlijk Sentinels project.

#7

Area i: Security and Privacy in e-Government/e-Business**Titel: Secure Smart Card Environments****Explanation: What is the problem?**

Tot nu toe is de burger vooral bekend met smart cards in de vorm van bankpassen en SIMs in mobiele telefoons. De komende jaren zullen smart cards verschijnen in veel andere situaties, zoals gezondheidszorg, openbaar vervoer, identiteitsbewijs (via PKI), etc. Hierbij zal het aantal kaartterminals (lezers) toenemen, en zal betrouwbaarheid van terminals een grotere rol gaan spelen. Ook zullen er aantrekkelijke killer-applicaties nodig zijn die het gebruik van smart cards liefst zonder dwang stimuleren (verg. met moeizame gewenning aan chipknip).

Industry and government: Who are faced with the problem?

Overheid, banken (inclusief Interpay met Finread initiatief), gezondheidszorg, openbaar vervoer, ...

Universities and knowledge institutes: Who can solve the problem?

TU/e, TUT, KUN vwb. securityprotocollen.

TNO

Further agreements: Who does what and when?

No further agreements at this moment.



#8

Area ii: Security and Privacy in Ambient Intelligence**Title: Security 4 E-Media****Explanation: What is the problem?**

In the digital age, the intrinsic limitations on content distribution have disappeared. Anyone can now make perfect copies of copyrighted digital content, which impacts the industrial parties and consumers in very different ways: From the content industry point of view illegal copying is theft; from the consumers point of view CDs and DVDs are too expensive. The IT and CE industry must cater for the needs of these two extremes...

Industry and government: Who are faced with the problem?

Philips, Chess

Universities and knowledge institutes: Who can solve the problem?

UT, TU/e, TUD, VU

Further agreements: Who does what and when?

UT, TU/e, TUD, VU will develop a proposal for novel content sharing systems.

#9

Area ii: Security and Privacy in Ambient Intelligence**Title: Ambient Privacy****Explanation: What is the problem?**

- Road pricing systems: Auto organising dynamic tariffs
- Traffic safety: "Car talk", swarms of communicating cars for the purpose of traffic safety, route planning dynamically, collecting traffic data

Further issues:

- (VU) Suppose all devices in a hospital (like MRI scanners) send data out to databases by wireless.
- (RWS) Finegrained democracy, small scale referenda on the fly
- (KUN) Privacy protection in ambient worlds
- (RUG) Personalised tokens; privacy vs. information needs

Industry and government: Who are faced with the problem?

Rijkswaterstaat,
Philips (Medical Systems)

Universities and knowledge institutes: Who can solve the problem?

KUN, TUD, UT

Further agreements: Who does what and when?

No further agreements at this moment.



#10

Area ii: Security and Privacy in Ambient Intelligence

Title: Policy Management for Dynamic Networks

Explanation: What is the problem?

- Ad hoc networks in which new devices enter/participate
- Evolving systems of intelligent devices -> maintaining security policy
- Consistent security policy over different networks

Industry and government: Who are faced with the problem?

Nedap;
Chess

Universities and knowledge institutes: Who can solve the problem?

KUN, VU

Further agreements: Who does what and when?

No further agreements at this moment.

#11

Area ii: Security and Privacy in Ambient Intelligence

Title: Agents in a local environment

Explanation: What is the problem?

Traditionally agents collected information from central institutions. Now the travel around in the local/personal environment of others; how to protect them against these 'rogue'/non-institutionalised environments, and how to protect these environments against hostile agents

Industry and government: Who are faced with the problem?

TNO;
KPN

Universities and knowledge institutes: Who can solve the problem?

KUN, VU

Further agreements: Who does what and when?

No further agreements at this moment.