UNIVERSITÄT KOBLENZ · LANDAU
Institut für Informatik

FB 4 Informatik

A Public Key Infrastructure in Ambient Information and Transaction Systems

Sebastian Magnus
Markus Maron

Nr. 11/2009

Arbeitsberichte aus dem Fachbereich Informatik

Arbeitsberichte des Fachbereichs Informatik

ISSN (Print): 1864-0346
ISSN (Online): 1864-0850

Herausgeber / Edited by:

Der Dekan:
Prof. Dr. Zöbel

Kontaktdaten der Verfasser

Sebastian Magnus, Markus Maron
Institut für Informatik
Fachbereich Informatik
Universität Koblenz-Landau
Universitätsstraße 1
D-56070 Koblenz
EMail: smagnus@uni-koblenz.de, maron@uni-koblenz.de

A Public Key Infrastructure in Ambient Information and Transaction Systems

Sebastian Magnus, Markus Maron
Universität Koblenz-Landau, Koblenz, Germany
smagnus@uni-koblenz.de, maron@uni-koblenz.de

10. August 2009

Zusammenfassung

Conventional security infrastructures in the Internet cannot be directly adopted to ambient systems, especially if based on short-range communication channels: Personal, mobile devices are used and the participants are present during communication, so privacy protection is a crucial issue. As ambient systems cannot rely on an uninterrupted connection to a Trust Center, certified data has to be verified locally. Security techniques have to be adjusted to the special environment. This paper introduces a public key infrastructure (PKI) to provide secure communication channels with respect to privacy, confidentiality, data integrity, non-repudiability, and user or device authentication. It supports three certificate levels with a different balance between authenticity and anonymity. This PKI is currently under implementation as part of the iCity project.

1 Introduction

Ambient intelligence systems enable to automatically connect mobile computing devices with environmental information. Such systems do not only evaluate location-dependent data, but also other context information like knowledge about the receiver, his interests or behavior. Because personalized information is linked with private data that might need protection, transactional security and privacy are major issues.
In the scope of the research project iCity [1], we are working on ambient intelligence systems in the field of mobile information and transaction services, which is often related to mobile business. Mobile devices with computational capabilities like smartphones or PDAs are used in different scenarios to support their users with personalized, location-dependent and time-dependent services. The project is in public transport for ticketing and timetable information, in mobile advertisement, and in healthcare for prescription information. To avoid charges by Mobile Network Operators, connections use the short-range wireless communication radio Bluetooth.

To provide security especially on the last meter and to protect private data, we developed a public key infrastructure (PKI). The PKI provides secure communication channels with respect to privacy, confidentiality, data integrity, non-repudiability, and user or device authentication. It supports three certificate levels with a different balance between authenticity and anonymity. This PKI is currently under implementation as part of the iCity project.
The paper describes a security concept which is under development within the iCity project. Adjustable to various scenarios, different levels of anonymity or authenticity are supported.
Before we introduce our PKI, we propose some example applications in Section 2 and discuss related work 3. Section 4 sketches the PKI for providing user authentication, integrity and secure data channels without unnecessary disruption of privacy. As described in 5 and 6, the PKI balances between privacy and non-repudiability by use of different certificates issued by a common Trust Center (TC). The interaction protocol is introduced in Section 7. We conclude in Section 8 with how to apply the PKI in particular scenarios.

2 Daily-life Scenarios

iCity is tested together with our business partners in outdoor advertising, public transport, and health care. Herein, we identified three typical daily-life service types to exemplify the usage of our PKI concept:

2.0.1 Anonymous Information Services:

Anonymous information services can be used for advertisement, tourist information, or timetable information in public transport. The identity of the customer is not relevant for the service provider, he may stay anonymous. In contrast, the provider's identity is public and has to be authenticated to prevent fraudsters from claiming the provider's identity as their own and to protect the customer from phishing or social engineering.

2.0.2 Registered or Context Sensitive Services:

The second class of applications are services which correspond to a certain context, for example the result of a former transaction or a particular, but not identified user. Typical registered services are anonymous but customized services and prepaid accounts.

2.0.3 Personal Services:

Financial and legal transactions often require the identification of a natural or legal person. Either partner needs to authenticate the counterpart. The communication often has to be non-repudiable in both directions, for example to comply with legal requirements. Because sensitive data are transmitted, protection against forgery and eavesdropping is crucial.

If participants are able to register with their partner, they could transmit and verify their personal data and simplify the transaction to a registered service. If the participants meet for the first time or if it is not possible to verify the data received earlier, the users have to be authenticated during link connection.

3 Background and Related Work

Security is a set of properties which are closely linked to a certain scenario. Depending on the concrete application, different characteristics may be required or undesired. Our PKI proposes a combination of different certificate types to be adaptable to various scenarios and balance between privacy and non-repudiability.
Security provided by current short-range media like Bluetooth and WLAN provide only limited security features: Bluetooth and WLAN support only point-to-point security [2, 3] with known vulnerabilities to its cryptography (e.g., see [4, 5] for Bluetooth and [6] for WLAN), mostly due to incomplete or incorrect implementation. Neither Bluetooth nor WLAN provide user authentication or non-repudiability.
Public key infrastructures are well-known approaches for key management and key distribution with aid of a central, trustworthy authority. Detailed overviews can be found in [7, 8]. However, these Internet-based approaches do not consider privacy: Participants are either trustworthy or not. In an ambient systems with interacting natural persons, both privacy and authentication are required.
To avoid those shortcomings, iCity implements a PKI on application layer. A proof-of concept in Java using Bluetooth-connections is currently under development. One major aspect of our PKI is an adaptable trade-off between privacy and non-repudiability. Privacy has to be protected either to comply with statutory regulations, or to retain user acceptance [9, 10]. To the contrary, some transaction require user authentication (e.g., for access control) and non-repudiability (e.g., for financial or legal transactions [11, 12]).
The iCity PKI is based on reliable security technologies. Asymmetric RSA cryptography [13] is used to protect the communication channel against eavesdropping and manipulation. Keys are provided by certificates similar to those defined in FIPS 186-2 Digital Signature Standard [14] or by publications of the German Federal Network Agency [15, 16, 17]. In contrast to those specification, iCity supports certificates for both the authentication of the owner and for anonymous, privacy-compliant services.
Security in iCity is based on asymmetric cryptography [13]. Sender A sends a message M to receiver B. After encryption with a function $c(M, K^B_{Pub})$ using a public key K^B_{Pub}, M can only be deciphered by the owner B of the corresponding private key K^B_{Priv}.
Integrity, authenticity, and non-repudiability is achieved by the use of digital signatures $S(M, A) = c(h(M), K^A_{Priv})$ which are the encrypted hash-value $h(M)$ of a message M [14]. A cryptographic hash function is a one-way function which maps messages of arbitrary length onto a representation of constant length. The

values are stochastically independent and uniformly distributed. It is not possible to efficiently create a message that fits to a certain value. Everyone can check if the message was manipulated by testing if $h(M) = c(S(M, A), K^A_{Pub})$. Only the owner A of the corresponding private key K^A_{Pub} is able to create such a signature.

4 Global PKI Scheme

The next sections describes the global interaction scheme of the iCity PKI as visualized in Figure 1. Participants are henceforth referred to as operators

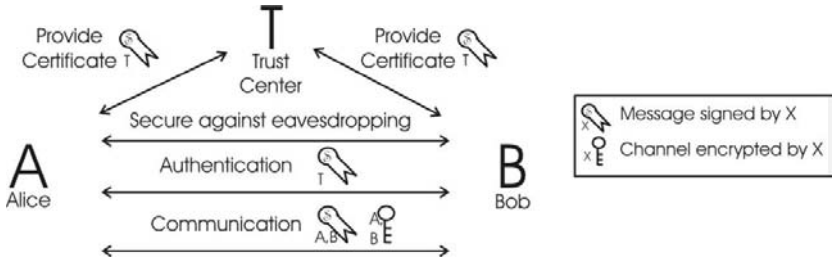

Abbildung 1: Interaction within the PKI

$O \in \{A, B, T\}$ with a Trust Center T, a sender A, and a recipient B. A and B want to transfer a message M. Every operator has at least one key pair with a public key K^O_{Pub} and a private key K^O_{Priv}.
T can certify the ownership of a key pair and additional information by signing the data D with a signature $S(D, T)$. A certificate $C^D = (D, S(D, T)))$ is created, which contains at least the public key K^O_{Pub} of its owner O and a certificate ID. Additional contents are described in Section 5.
The TC is used as a central authority which is trustworthy to all participants with respect to the correct creation of certificates. Everyone can locally verify the TC's signature by use of its public key K^T_{Pub}.

5 Certificates in iCity

iCity uses certificates to enable key exchange, authentication, non-repudiability, and to support protection against eavesdropping and forgery. This section introduces three types of certificates as shown in Fig. 2: Ad-Hoc Certificates, Anonymous Certificates, and Personalized Certificates. Each class supports a different trade-off between privacy and non-repudiability. Authentication and non-repudiability is achieved by extending anonymous certificates with additional data.

Abbildung 2: Certificates in iCity

5.0.4 Ad-Hoc Certificate (AHC):

Ad-Hoc Certificates (AHC) are completely anonymous certificates created by its owner himself that contain only cryptographic information. Its creator could claim any content, therefore AHCs only provide protection against eavesdropping, but not against masquerade or MITM-attacks.
AHCs are applicable if communication requires protection against eavesdropping, but not identification of the receiver. Another scenario for AHCs is the privacy-protecting exchange of higher-level certificates. In contrast to Internet-scenarios, the owner is visibly present in ambient systems. Eavesdroppers could create a link between the natural person and personal data in the certificate. By previously protecting the connection with an AHC, higher-level certificates can be submitted exclusively to the communication partner.
Notwithstanding the general definition in Section 4, AHCs are the only certificates which are not signed, because they are not created by a TC. Technically, they are rather a set of cryptographic information than a certificate.

5.0.5 Anonymous Certificate (AC):

Anonymous Certificates (AC) contain the same cryptographic information as the AHC and additional administrative information as well as a TC signature. The signature can only be created by the TC and proves the integrity of the content: Everyone can verify the certificate via the TC's public key. In particular, the TC certifies the ownership of a key pair by signing a public key contained in the certificate. ACs do not contain any personal information, therefore the recipient cannot identify the owner solely by the certificate, but he can recognize the unique certificate ID-number and see if he already communicated with the participant. The owner may possess more than one AC to hide links between independent transactions.

5.0.6 Personalized Certificate (PC):

The former two certificates are not able to personally identify its owner. In many scenarios, it is not enough to identify the certificate. Customers should always be able to identify companies, and it may be required to identify natural

persons to lower a payee's risk of non-payment, to verify access rights, or to support legal transactions.
Personalized Certificates contain all data already mentioned for ACs, but also additional personal data. They require at least the name and address of the owner and a personal identification characteristic. This could be the identification card number for natural persons. These data have to be verified by the TC during certification.
By using a PC, the participant gives up his anonymity. Therefore, the user is asked for a PIN for the PC's transmission. A natural person's PC is only transfered if it is required for the transaction, and if the client can trust the receiver of the certificate with respect to privacy protection.
Note that PCs are not always required to certify the user's identity. Instead, it is possible to identify the participant with data verified in prior transactions and linked to an AC.

6 Content of iCity Certificates

This section describes data contained in the certificates. Table 1 summarizes the entries. The data are partitioned into four sections: Header data, cryptographic information, administrative information, and data about the owner.

Header Data (AHC, AC, PC)	
Type	Type of Certificate [AHC | AC | PC].
Certificate ID	Identification number of the certificate. TC-wide unique in AC and PC. Not unique in AHC.
Cryptographic Information (AHC, AC, PC)	
$c()$	Name of the cryptographic algorithm $c()$.
K_{Pub}	Public key of the certificate owner.
$h()$	Name of the hash-function $h()$.
Administrative Information (AC, PC)	
Expiry date	The certificate is not valid after that date.
Issuer	Name and URL of the issuing TC.
$S(C, K^T_{Priv})$	Signature $S(C, K^T_{Priv}) = c(h(C), K^T_{Priv})$ of the issuing TC.
Owner Data (PC)	
Writer	ID of the TC-employee who issued the certificate. The ID is a pseudonym only known to the TC.
ID	Type and value of the presented identification characteristic (e.g., identity card).
Owner	Name and Address of the certificate owner (Natural person or company).

Tabelle 1: Data of the Certificate

6.0.7 Header Data:

These data are used to identify the certificate and its type. The Certificate ID is unique within one issuing TC, respectively for AHCs on one device. In AHCs, the ID keeps constant within one communication. In ACs and PCs, it always keeps constant and can be used to recognize a communication partner from earlier communications.

6.0.8 Cryptographic Information:

The data of this class are required to build up a tap-proof connection to the certificate owner A and to verify the authenticity of messages M sent by A. It contains the public key K^A_{Pub} of the owner as well as the name of the hash- and cipher-algorithms $h()$ and $c()$. The corresponding private key is never transmitted, not even to or from the Trust Center.
The key is used to encrypt messages which can only be decrypted by A with the corresponding private key, and attach a signature to messages sent by A.
The cryptographic function works only in one direction. To establish a bidirectional channel, one certificate is required for every participant.

6.0.9 Administrative Information:

The second information block contributes data about the issuing Trust Center and the expiry of the certificate. The name of the TC is used to determine which pre-known public key has to be used to verify the certificate. The block also contains the issuing TC's signature which certifies the data. Everyone can check it by use of the TC's public key.
A certificate is invalid if the current date is after the expiry date. The certificate is afterwards only used to verify stored messages, for example to prove the content and participants of a former transaction.

6.0.10 Data about the owner:

In some applications, the participants have to be identified as natural persons or companies, especially if contracts are to be signed or during financial transactions. Moreover, a customer has to identify the provider of an access point to be protected from phishing or masqueraders. For this purpose, additional data about the owner can be certified in PCs.
Owner data contains at least the name of the owner, an identification characteristic (e.g., his identification card number), and his current postal address. It can optionally contain contact information, like phone number, E-Mail address, or web URL.
Generating a certificate with owner data is more complex than producing an AC, since the correctness of the certified data has to be verified by the issuing TC. This is not always possible without physical interaction.

7 Link Connection and Data Exchange

By use of the infrastructure above, a secure communication channel between two participants can be established. This section explains the link connection and communication protocol. The particular steps are described in more detail in the subsections. The channel is secured by the following steps:

1. Securing the channel against eavesdropping
2. Authentication
3. Communication

7.0.11 Securing the channel against eavesdropping:

The communication channel is at first secured only against eavesdropping and message manipulation. The securing process takes one optional and one mandatory step for each direction:

1. Ad-Hoc Certificate Generation (if required)
2. Certificate Exchange

In most scenarios, the channel will protect the communication between a natural person and a service provider. While the service provider's identity is in general not private and a PC can be transferred on an unsecured channel, the customer has a right for privacy. He generates a key pair and the corresponding AHC to protect the channel against eavesdropping. A natural person's AC or PC is only transmitted when it is required for authentication and only on a tap-proof channel.
Every participant manages his certificates by himself, the TC is not required for certificate exchange or verification. When a connection is established, the participants submit their certificate to the communication partner.
Certificates can only be used if the current date is before the expiry date. Out-of-date certificates can be stored to prove former communications, but not for encrypting messages.

7.0.12 Authentication:

If a natural person connects with a service provider, the service provider submits his certificate first, his identity is not confidential. If the customer requires an AC or PC, it is transfered second to be sure to submit it to the right partner. The authentication takes three steps per direction:

1. Exchange of AC or PC (If required)
2. Local verification of certificate
3. Verification of communication partner

If not done in the step mentioned above, a certificate of the correct type (AC or PC) is submitted. The certificate C of participant A is checked by its receiver locally by testing the signature via the TC's pre-known public key and hash-function: $c(S(C,A),K^T_{Pub}) = h(C)$
The certificate could be recorded during a previous communication, so testing the signature is not sufficient to recognize the communication partner. An attacker who repeats a foreign certificate could neither sign his own messages nor read received messages, but the partner could not notice the difference to a disturbed connection. For this reason, the communication partners are tested bidirectionally with help of two random numbers:
One participant A generates a random number n_1 and sends it to his communication partner B. B appends bit by bit a second random number n_2, producing a new number n. He encrypts the number by using his private key: $n^{K^B_{Priv}} = c(n,K^B_{Priv})$. $n^{K^B_{Priv}}$ is sent to A, who decrypts the number $n' = c(n,K^B_{Pub})$. B is really the owner of the key pair noted in the certificate if n_1 is contained in n.
To verify his own certificate, A now encrypts n by use of his private key K^A_{Priv} and sends the number back to B. B decrypts the number with help of K^A_{Pub} and checks if n_2 is contained in the number.
The number is constructed of two parts to ensure the authentication cannot be abused as an oracle. Neither A nor B can chose n alone and therefore are not able to make the partner en- or decrypt arbitrary messages in the length of the numbers. Authenticating the participants bidirectionally is also more efficient than repeating a unidirectional authentication.
The random number n is memorized for later, it is needed as a serial number during communication.

7.0.13 Communication:

At this point, a secure channel between A and B is established. The cryptographic data contained in the certificate are used to encrypt messages. The following protocol is used in both directions:

- A: Increase serial number n by one, append to message
- A: Sign message: $S(M^{K^B_{Pub}},A) = c(h(M^{K^B_{Pub}}),K^A_{Priv})$
- A: Encrypt message with $M^{K^B_{Pub}} = c(M,K^B_{Pub})$
- A: Send message
- B: Decrypt Message $M = c(M^{K^B_{Pub}},K^B_{Priv})$
- B: Test signature: $h(M^{K^B_{Pub}}) = c(S(M^{K^B_{Pub}},A),K^A_{Pub})$
- B: Check serial number
- B: Send acknowledgement

A serial number is appended at the beginning of the message to prevent repeater attacks. Hence this number changes with every message and is known only to the participants, recording and repeating would result in infeasible messages. The random number n from the authentication process is used as initial serial number, for every subsequent message the number is increased by one.
The message is signed via the sender's private key K^A_{Priv} and encrypted together with the signature using the public key of the receiver K^B_{Pub}. The resulting message is sent to the receiver, who decrypts it and checks the signature as well as the serial number.
To check if the messages are received correctly, the receiver sends back the signed serial number, which also is used as an acknowledgement for non-repudiability.

8 Applying the PKI in Daily-Life Scenarios

We already mentioned some sample applications in Section 2. Here we explain how the iCity PKI can be applied to those scenarios.

8.0.14 Information Services:

The service provider sends a PC to the customer to authenticate himself and protect customers from phishing or other abuse. The provider's certificate is submitted first, since it does only contain public data. The customer answers with an AHC to protect the channel against eavesdropping without publishing personal information.

8.0.15 Registered or Context Sensitive Services:

The service provider begins authentication with a PC. The customer answers with an AC to create a link to his account respectively the correct context.

8.0.16 Personal Services:

If information about the natural person is required, both partners use a PCs. If one participant is a service provider or company, his certificate is transmitted first, the natural person's certificate second. If both partners are natural persons, they have to decide who starts. The person is always prompted for a PIN before submitting his personal data to proof that no third person is using his mobile device and to confirm the abandoning of anonymity.

9 Conclusion

The proposed PKI enables bug-proof, non-repudiable end-to-end communication with user and data authentication. Different security levels either provide a high degree of anonymity or allow personal authentication. Only public information is exchanged via an unsecured channel. No connection to a Trust Center

is needed during link connection.
The concept considers how to achieve the security requirements of typical ambient system scenarios. However, efficiency was not investigated yet. Future extensions will explore the integration of symmetric cryptography, for example how to exchange symmetric keys on the tap-proof channel combined with asymmetric signatures.

Acknowledgment

The authors would like to thank their industry partners, the Ministry of Rhineland-Palatinate and EFRE who are founders of the iCity project.

Literatur

[1] University of Koblenz, AGKI: iCity-a research project on ambient Intelligence System (Online; 2009-06-07) www.uni-koblenz.de/icity

[2] National Institute of Standards and Technology - U.S. Department of Commerce: Guide to Bluetooth Security. Special Publication **800-121** (September 2008)

[3] National Institute of Standards and Technology, U.S. Department of Commerce: Wireless network security - 802.11, bluetooth and handheld devices. Special Publication **800-48** (November 2002)

[4] Wool, A., yaniv Shaked: Cracking the bluetooth pin. In Proc. 3rd USENIX/ACM Conf. Mobile Systems, Applications, and Services (MobiSys) **3** (June 2005) 39–50

[5] Lu, Y., Meier, W., Vaudenay, S.: The conditional correlation attack: A practical attack on bluetooth encryption. Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference **3621** (2005) 97–117

[6] Chaabouni, R.: Break WEP Faster with Statistical Analysis. Technical Report, EPFL, LASEC (June 2006)

[7] Schmeh, K.: Kryptografie – Verfahren, Protokolle, Infrastrukturen. Volume 3. dpunkt.verlag (2007)

[8] Buchmann, J.: Einführung in die Kryptographie. Volume 4. Springer-Verlag Berlin Heidelberg (2008)

[9] Bundesministerium der Justiz: Bundesdatenschutzgesetz (bdgs). (August 2006)

[10] Becher, S., Laue, P., Maidl, M., Modsching, M.: Die Datenschutz- und sicherheitskonforme Ausgestaltung von Location Based Services am Beispiel eines mobilen Touristenführers. Mobilität und mobile Informationssysteme 2007 (MMS) (March 2007) 86–96

[11] Phan, T.T.H., Dang, T.K.: An Extended Payment Model with Fair Non-Repudiation Protocols for M-Commerce. In: MoMM'2007 - The Fifth International Conference on Advances in Mobile Computing and Multimedia. (2007) 227–232

[12] Hiltgen, A., Kramp, T., Weigold, T.: Secure Internet Banking Authentication. IEEE Security & Privacy **4**(2) (March 2006) 21–29

[13] Rivest, R.L., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM **21** (1978) 120–126

[14] U.S. Department of Commerce, National Institute of Standards and Technology: Digital Signature Standard (DSS). Federal Information Processing Standards Publication (186-2) (January 2000)

[15] Bundesnetzagentur: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten. **1.4** (July 2005)

[16] Bundesnetzagentur: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen). Bundesanzeiger (13) (January 2009) 346 – 257

[17] Giessmann, E., Lippert, M., Bundesnetzagentur, T-Systems: Trustcenter Bundesnetzagentur – Realisierung Übersignaturkomponente. **2** (March 2008)

Bisher erschienen

Arbeitsberichte aus dem Fachbereich Informatik

(http://www.uni-koblenz.de/fb4/publikationen/arbeitsberichte)

Sebastian Magnus, Markus Maron, A Public Key Infrastructure in Ambient Information and Transaction Systems, Arbeitsberichte aus dem Fachbereich Informatik 11/2009

Ammar Mohammed, Ulrich Furbach, Multi-agent systems: Modeling and Virification using Hybrid Automata, Arbeitsberichte aus dem Fachbereich Informatik 10/2009

Andreas Sprotte, Performance Measurement auf der Basis von Kennzahlen aus betrieblichen Anwendungssystemen: Entwurf eines kennzahlengestützten Informationssystems für einen Logistikdienstleister, Arbeitsberichte aus dem Fachbereich Informatik 9/2009

Gwendolin Garbe, Tobias Hausen, Process Commodities: Entwicklung eines Reifegradmodells als Basis für Outsourcingentscheidungen, Arbeitsberichte aus dem Fachbereich Informatik 8/2009

Petra Schubert et. al., Open-Source-Software für das Enterprise Resource Planning, Arbeitsberichte aus dem Fachbereich Informatik 7/2009

Ammar Mohammed, Frieder Stolzenburg, Using Constraint Logic Programming for Modeling and Verifying Hierarchical Hybrid Automata, Arbeitsberichte aus dem Fachbereich Informatik 6/2009

Tobias Kippert, Anastasia Meletiadou, Rüdiger Grimm, Entwurf eines Common Criteria-Schutzprofils für Router zur Abwehr von Online-Überwachung, Arbeitsberichte aus dem Fachbereich Informatik 5/2009

Hannes Schwarz, Jürgen Ebert, Andreas Winter, Graph-based Traceability – A Comprehensive Approach. Arbeitsberichte aus dem Fachbereich Informatik 4/2009

Anastasia Meletiadou, Simone Müller, Rüdiger Grimm, Anforderungsanalyse für Risk-Management-Informationssysteme (RMIS), Arbeitsberichte aus dem Fachbereich Informatik 3/2009

Ansgar Scherp, Thomas Franz, Carsten Saathoff, Steffen Staab, A Model of Events based on a Foundational Ontology, Arbeitsberichte aus dem Fachbereich Informatik 2/2009

Frank Bohdanovicz, Harald Dickel, Christoph Steigner, Avoidance of Routing Loops, Arbeitsberichte aus dem Fachbereich Informatik 1/2009

Stefan Ameling, Stephan Wirth, Dietrich Paulus, Methods for Polyp Detection in Colonoscopy Videos: A Review, Arbeitsberichte aus dem Fachbereich Informatik 14/2008

Tassilo Horn, Jürgen Ebert, Ein Referenzschema für die Sprachen der IEC 61131-3, Arbeitsberichte aus dem Fachbereich Informatik 13/2008

Thomas Franz, Ansgar Scherp, Steffen Staab, Does a Semantic Web Facilitate Your Daily Tasks?, Arbeitsberichte aus dem Fachbereich Informatik 12/2008

Norbert Frick, Künftige Anfordeungen an ERP-Systeme: Deutsche Anbieter im Fokus, Arbeitsberichte aus dem Fachbereicht Informatik 11/2008

Jürgen Ebert, Rüdiger Grimm, Alexander Hug, Lehramtsbezogene Bachelor- und Masterstudiengänge im Fach Informatik an der Universität Koblenz-Landau, Campus Koblenz, Arbeitsberichte aus dem Fachbereich Informatik 10/2008

Mario Schaarschmidt, Harald von Kortzfleisch, Social Networking Platforms as Creativity Fostering Systems: Research Model and Exploratory Study, Arbeitsberichte aus dem Fachbereich Informatik 9/2008

Bernhard Schueler, Sergej Sizov, Steffen Staab, Querying for Meta Knowledge, Arbeitsberichte aus dem Fachbereich Informatik 8/2008

Stefan Stein, Entwicklung einer Architektur für komplexe kontextbezogene Dienste im mobilen Umfeld, Arbeitsberichte aus dem Fachbereich Informatik 7/2008

Matthias Bohnen, Lina Brühl, Sebastian Bzdak, RoboCup 2008 Mixed Reality League Team Description, Arbeitsberichte aus dem Fachbereich Informatik 6/2008

Bernhard Beckert, Reiner Hähnle, Tests and Proofs: Papers Presented at the Second International Conference, TAP 2008, Prato, Italy, April 2008, Arbeitsberichte aus dem Fachbereich Informatik 5/2008

Klaas Dellschaft, Steffen Staab, Unterstützung und Dokumentation kollaborativer Entwurfs- und Entscheidungsprozesse, Arbeitsberichte aus dem Fachbereich Informatik 4/2008

Rüdiger Grimm: IT-Sicherheitsmodelle, Arbeitsberichte aus dem Fachbereich Informatik 3/2008

Rüdiger Grimm, Helge Hundacker, Anastasia Meletiadou: Anwendungsbeispiele für Kryptographie, Arbeitsberichte aus dem Fachbereich Informatik 2/2008

Markus Maron, Kevin Read, Michael Schulze: CAMPUS NEWS – Artificial Intelligence Methods Combined for an Intelligent Information Network, Arbeitsberichte aus dem Fachbereich Informatik 1/2008

Lutz Priese,Frank Schmitt, Patrick Sturm, Haojun Wang: BMBF-Verbundprojekt 3D-RETISEG Abschlussbericht des Labors Bilderkennen der Universität Koblenz-Landau, Arbeitsberichte aus dem Fachbereich Informatik 26/2007

Stephan Philippi, Alexander Pinl: Proceedings 14. Workshop 20.-21. September 2007 Algorithmen und Werkzeuge für Petrinetze, Arbeitsberichte aus dem Fachbereich Informatik 25/2007

Ulrich Furbach, Markus Maron, Kevin Read: CAMPUS NEWS – an Intelligent Bluetooth-based Mobile Information Network, Arbeitsberichte aus dem Fachbereich Informatik 24/2007

Ulrich Furbach, Markus Maron, Kevin Read: CAMPUS NEWS - an Information Network for Pervasive Universities, Arbeitsberichte aus dem Fachbereich Informatik 23/2007

Lutz Priese: Finite Automata on Unranked and Unordered DAGs Extented Version, Arbeitsberichte aus dem Fachbereich Informatik 22/2007

Mario Schaarschmidt, Harald F.O. von Kortzfleisch: Modularität als alternative Technologie- und Innovationsstrategie, Arbeitsberichte aus dem Fachbereich Informatik 21/2007

Kurt Lautenbach, Alexander Pinl: Probability Propagation Nets, Arbeitsberichte aus dem Fachbereich Informatik 20/2007

Rüdiger Grimm, Farid Mehr, Anastasia Meletiadou, Daniel Pähler, Ilka Uerz: SOA-Security, Arbeitsberichte aus dem Fachbereich Informatik 19/2007

Christoph Wernhard: Tableaux Between Proving, Projection and Compilation, Arbeitsberichte aus dem Fachbereich Informatik 18/2007

Ulrich Furbach, Claudia Obermaier: Knowledge Compilation for Description Logics, Arbeitsberichte aus dem Fachbereich Informatik 17/2007

Fernando Silva Parreiras, Steffen Staab, Andreas Winter: TwoUse: Integrating UML Models and OWL Ontologies, Arbeitsberichte aus dem Fachbereich Informatik 16/2007

Rüdiger Grimm, Anastasia Meletiadou: Rollenbasierte Zugriffskontrolle (RBAC) im Gesundheitswesen, Arbeitsberichte aud dem Fachbereich Informatik 15/2007

Ulrich Furbach, Jan Murray, Falk Schmidsberger, Frieder Stolzenburg: Hybrid Multiagent Systems with Timed Synchronization-Specification and Model Checking, Arbeitsberichte aus dem Fachbereich Informatik 14/2007

Björn Pelzer, Christoph Wernhard: System Description:"E-KRHyper", Arbeitsberichte aus dem Fachbereich Informatik, 13/2007

Ulrich Furbach, Peter Baumgartner, Björn Pelzer: Hyper Tableaux with Equality, Arbeitsberichte aus dem Fachbereich Informatik, 12/2007

Ulrich Furbach, Markus Maron, Kevin Read: Location based Informationsystems, Arbeitsberichte aus dem Fachbereich Informatik, 11/2007

Philipp Schaer, Marco Thum: State-of-the-Art: Interaktion in erweiterten Realitäten, Arbeitsberichte aus dem Fachbereich Informatik, 10/2007

Ulrich Furbach, Claudia Obermaier: Applications of Automated Reasoning, Arbeitsberichte aus dem Fachbereich Informatik, 9/2007

Jürgen Ebert, Kerstin Falkowski: A First Proposal for an Overall Structure of an Enhanced Reality Framework, Arbeitsberichte aus dem Fachbereich Informatik, 8/2007

Lutz Priese, Frank Schmitt, Paul Lemke: Automatische See-Through Kalibrierung, Arbeitsberichte aus dem Fachbereich Informatik, 7/2007

Rüdiger Grimm, Robert Krimmer, Nils Meißner, Kai Reinhard, Melanie Volkamer, Marcel Weinand, Jörg Helbach: Security Requirements for Non-political Internet Voting, Arbeitsberichte aus dem Fachbereich Informatik, 6/2007

Daniel Bildhauer, Volker Riediger, Hannes Schwarz, Sascha Strauß, „grUML – Eine UML-basierte Modellierungssprache für T-Graphen", Arbeitsberichte aus dem Fachbereich Informatik, 5/2007

Richard Arndt, Steffen Staab, Raphaël Troncy, Lynda Hardman: Adding Formal Semantics to MPEG-7: Designing a Well Founded Multimedia Ontology for the Web, Arbeitsberichte aus dem Fachbereich Informatik, 4/2007

Simon Schenk, Steffen Staab: Networked RDF Graphs, Arbeitsberichte aus dem Fachbereich Informatik, 3/2007

Rüdiger Grimm, Helge Hundacker, Anastasia Meletiadou: Anwendungsbeispiele für Kryptographie, Arbeitsberichte aus dem Fachbereich Informatik, 2/2007

Anastasia Meletiadou, J. Felix Hampe: Begriffsbestimmung und erwartete Trends im IT-Risk-Management, Arbeitsberichte aus dem Fachbereich Informatik, 1/2007

„Gelbe Reihe"
(http://www.uni-koblenz.de/fb4/publikationen/gelbereihe)

Lutz Priese: Some Examples of Semi-rational and Non-semi-rational DAG Languages. Extended Version, Fachberichte Informatik 3-2006

Kurt Lautenbach, Stephan Philippi, and Alexander Pinl: Bayesian Networks and Petri Nets, Fachberichte Informatik 2-2006

Rainer Gimnich and Andreas Winter: Workshop Software-Reengineering und Services, Fachberichte Informatik 1-2006

Kurt Lautenbach and Alexander Pinl: Probability Propagation in Petri Nets, Fachberichte Informatik 16-2005

Rainer Gimnich, Uwe Kaiser, and Andreas Winter: 2. Workshop "Reengineering Prozesse" – Software Migration, Fachberichte Informatik 15-2005

Jan Murray, Frieder Stolzenburg, and Toshiaki Arai: Hybrid State Machines with Timed Synchronization for Multi-Robot System Specification, Fachberichte Informatik 14-2005

Reinhold Letz: FTP 2005 – Fifth International Workshop on First-Order Theorem Proving, Fachberichte Informatik 13-2005

Bernhard Beckert: TABLEAUX 2005 – Position Papers and Tutorial Descriptions, Fachberichte Informatik 12-2005

Dietrich Paulus and Detlev Droege: Mixed-reality as a challenge to image understanding and artificial intelligence, Fachberichte Informatik 11-2005

Jürgen Sauer: 19. Workshop Planen, Scheduling und Konfigurieren / Entwerfen, Fachberichte Informatik 10-2005

Pascal Hitzler, Carsten Lutz, and Gerd Stumme: Foundational Aspects of Ontologies, Fachberichte Informatik 9-2005

Joachim Baumeister and Dietmar Seipel: Knowledge Engineering and Software Engineering, Fachberichte Informatik 8-2005

Benno Stein and Sven Meier zu Eißen: Proceedings of the Second International Workshop on Text-Based Information Retrieval, Fachberichte Informatik 7-2005

Andreas Winter and Jürgen Ebert: Metamodel-driven Service Interoperability, Fachberichte Informatik 6-2005

Joschka Boedecker, Norbert Michael Mayer, Masaki Ogino, Rodrigo da Silva Guerra, Masaaki Kikuchi, and Minoru Asada: Getting closer: How Simulation and Humanoid League can benefit from each other, Fachberichte Informatik 5-2005

Torsten Gipp and Jürgen Ebert: Web Engineering does profit from a Functional Approach, Fachberichte Informatik 4-2005

Oliver Obst, Anita Maas, and Joschka Boedecker: HTN Planning for Flexible Coordination Of Multiagent Team Behavior, Fachberichte Informatik 3-2005

Andreas von Hessling, Thomas Kleemann, and Alex Sinner: Semantic User Profiles and their Applications in a Mobile Environment, Fachberichte Informatik 2-2005

Heni Ben Amor and Achim Rettinger: Intelligent Exploration for Genetic Algorithms – Using Self-Organizing Maps in Evolutionary Computation, Fachberichte Informatik 1-2005