



EAB Newsletter

Edition April 2012

Editorial committee:

Georg Hasse

Max Snijder

contact: secretariat@eab.org

Production:

European Biometrics Group



Content

1. News from the EAB.....	3
From the EAB Chairman	3
EAB represented in the UK's Standardisation Committee for Biometrics	3
More information on the BSI Committee IST/44 Biometrics can be found through the following link:	4
http://standardsdevelopment.bsigroup.com/Home/Committee/50087978#tabs-representation	4
EAB to initiate joint event with NIST and Biometrics Institute on template protection	4
EAB has signed up partnerships with SDW and World eID	4
Privacy Impact Assessment Working Group: call for participation	4
Charter EAB Biometrics Advisory Council finalized and approved	4
EAB Biometrics Research Award: call for participants has opened	5
2. EU/EC/EP	5
Report on EDPS Peter Hustinx' speech given at the European Biometrics Symposium (by Juliet Lodge)	5
EC answers to critical questions Sophie In't Veld and Sarah Ludford (MEP's) on performance of Dutch biometric passport.....	7
French Constitutional Court rules against central storage of citizens' fingerprints.....	8
3. EU Projects	10
BEAT: Europe to invest in biometric testing and evaluation	10
Fidelity: addressing shortcomings and vulnerabilities in the ePassport life cycle in Europe.....	11
4. Academia.....	12
International cooperation: Carlos III University (Madrid) and the Purdue University (US) to develop BioAPI reference platforms	12
5. Industry & Projects	12
WCC chosen to power a traveler management system for the Ministry of Interior of the Republic of Estonia....	12
36 e-passport based ABC gates started at Schiphol Airport.....	13
German Border Police chooses secunet for the DVCA project	14
Opportunities for biometrics in the mobile market	14
European Biometrics Group to conduct a study for the European Parliament on the e-passport in Europe.....	15
6. Outside Europe.....	15
NIST publishes IREX III results	15
7. Events	16
IBPC 2012 Conference report	16
IBC 2012 Conference Report	16
EAB workshop "Transcontinental Perspectives on Privacy and Metrics for Biometric Template Protection" in cooperation with NIST and BI: Paris, Friday 13th July, 2012	17
Security Document World 2012: London, 21-23 May, 2012.....	17
BIOSIG 2012 conference: Darmstadt 6-7 September, 2012	17
World eID Conference: Nice, 17-21 September 2012	18

1. News from the EAB

From the EAB Chairman



"It is with great honor and pleasure that I am presenting to you the first EAB Newsletter. It is a landmark for the biometrics community in Europe as for the first time we can speak about a newsletter produced by the community for the community. It can be considered as a major step towards an improved mechanism of information exchange, bringing more coherence into the overall knowledge about biometrics in Europe. Through our network of members we are seeking for national, European and international news about developments in biometrics, ranging from academic achievements to policy developments and industrial breakthroughs. The EAB Newsletter should contribute to a better understanding of the many aspects that large scale deployment of biometrics concern. Next time we hope to receive your contributions again. I wish you a pleasurable and informative read."

Dr. Alexander Nouak, Chairman

EAB represented in the UK's Standardisation Committee for Biometrics

The UK's standardisation committee for biometrics (British Standards Institute IST/44) has invited a representative from EAB to serve on their committee. From the EAB Dr Farzin Deravi was appointed as its representative. He will act as liaison and rapporteur to the EAB. EAB chairman Alexander Nouak says:

"I fully appreciate this invitation by the UK BSI and I am very proud that EAB was granted representation on such an influential body. It should be noted that NIA37 of DIN recently concluded that better dissemination of the standards is vital. The EAB could be the perfect partner to collaborate on such tasks."

The UK's standardisation committee for biometrics (British Standards Institute IST/44) is working on the standardization of various aspects of biometric technology. Under the direction of the Standards Policy and Strategy Committee, the IST/44 Committee is responsible for the UK input to standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of



evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects. Excluded is the work in ISO/IEC JTC 1/SC 17 to apply biometric technologies to cards and personal identification. Excluded is the work in ISO/IEC JTC 1/SC 27 for biometric data protection techniques, biometric security testing, evaluations and evaluation methodologies.

More information on the BSI Committee IST/44 Biometrics can be found through the following link:

<http://standardsdevelopment.bsigroup.com/Home/Committee/50087978#tabs-representation>

EAB to initiate joint event with NIST and Biometrics Institute on template protection

The EAB is organizing a workshop "**Transcontinental Perspectives on Privacy and Metrics for Biometric Template Protection**". The event will take place in Paris on Friday, 13 July, 2012, and is co-located with ISO/IEC JTC1 SC37. See the 'Events' section on this newsletter for more information

EAB has signed up partnerships with SDW and World eID

The EAB has signed up partnership agreements with World eID and Security Document World (SDW). Both major events have agreed to exchange logo's and to provide mutual services, such as event announcements, special rates for EAB members and listing in the EAB events list.

Privacy Impact Assessment Working Group: call for participation

Recently the charter of the EAB Privacy Impact Assessment Working Group (PIA WG) has been approved by the EAB management board. That means that the WG can start its activities with calling EAB members to participate. The mission of the PIA-WG is to make an inventory on the existing work done at various levels and by various organizations regarding the development of PIA frameworks which are suitable to assess biometric applications and systems on their impact on privacy. In order to assess the relevance of existing work and best practices the WG will also get into the question, whether (and if yes: in what respect) biometric applications and systems do require special assessment methods and validation. The full charter of the PIA WG can be found at www.eab.org.

To apply for participation to the PIA WG please send a request to secretariat@eab.org.

Charter EAB Biometrics Advisory Council finalized and approved

The final version of the charter of the EAB Biometrics Advisory Council has been published on the EAB website. EABAC is the EAB's internal advisory council, as laid down by the EAB's



constitution. It consists of selected representatives from the wider biometrics and identity community, including from outside Europe. Members of the EABAC are nominated by EAB members at the General Assembly and appointed by the Management Board of the EAB. Nominations for potential EABAC members will be gladly received by the board.

EAB Biometrics Research Award: call for participants has opened

EAB is launching the sixth European Biometrics Research and Industry Award 2012. This prestigious award is granted annually to individuals who have been judged by a panel of internationally respected experts to be making a significant contribution to the field of biometrics research in Europe. The award is stimulating innovation in academic research as well as in industry. Thus biometric experts with either of the following profiles should submit their work. Academic researchers enrolled in the last or penultimate year of a Ph.D. program or who have obtained a Ph.D., with major focus on biometrics, from a European academic institution no later than two years before the given deadline, might consider applying for the award. Further industrial researchers employed by European companies whose core business is biometrics might consider applying for the award. The industry award will be granted to the candidate that has created the strongest impact for industry.

Applicants are asked to submit a research paper by June 30, 2012. For further information on the EAB awards and the application process please visit:

<http://www.eab.org/expertise/com/award.html>

You can also contact Partizio Campisi, chairman of the award, at campisi@uniroma3.it.

2. EU/EC/EP

Report on EDPS Peter Hustinx' speech given at the European Biometrics Symposium (by Juliet Lodge)

The Copernican Revolution in data handling

A report of Peter Hustinx' keynote presentation at the European Biometrics Symposium, 17th February 2012 Prof Dr Juliet Lodge

'Don't put a peeping Tom in charge of putting up your curtains', Peter Hustinx, the EU Data Protection Supervisor, once famously said. The EU Commission, in proposing a Regulation to replace and update the Directive on privacy and data protection has listened. For Hustinx, the proposed Regulation represents a Copernican revolution in data handling. Stressing that it has retained the basic principles and values underlying the current 15 year old Directive, he told the BEST Network that the draft Regulation had been updated to match the realities of a cyber driven world.

It is welcome for many reasons. First because, as a Regulation, it injects uniformity over the complexity, diversity and resultant discriminatory inequalities that result from EU 27 member governments implementing the Directive in very different ways with very different consequences for citizens. It takes direct effect. Member states cannot escape its requirements by re-interpreting it as they go about implementing it. Discrepancies remain across criminal law enforcement where revisions to replace a framework decision by a directive for criminal law enforcement lack consistent references to biometric data. But biometric data are covered by the requirements on data handling in the Regulation to ensure that there is effectiveness in practice in implementing and enforcing the legislation.

Second, the Regulation reflects the idea of the importance of citizens to sustaining integration and trust in government in the EU. It reflects the Lisbon Treaty's intention to put citizens at the heart of Europe. The Regulation intends to ensure that anyone handling EU citizens' data is required to comply with EU law on privacy and data protection, regardless of where they happen to be in the world or cyberspace.

The Regulation will make data controllers responsible for data flows. What does this mean? It means that the onus for proving that data has been collected and handled responsibly is placed on the data controller wherever located. The data controller is responsible for providing, on a case-by-case basis, reasons for collecting data in the first place. The tests are: Is the volume collected proportionate? Has the principle of data minimisation been observed? Has a privacy impact assessment been conducted and is it constantly updated to reflect technological innovation as legacy systems are updated? How long is data held? The data controller is responsible for giving procedural effect to the principle of a 'right to be forgotten' and so must be able to provide evidence to show that data can be and is deleted; that 'forgotten' allows someone to 'exit'. As Peter Hustinx explained, this means that youthful indiscretions on social networking sites should be deleted when the subject requests deletion or after the elapse of a short period of time.

In short, the Regulation also therefore gives substance to the principle of consent. Consent must be free, informed, specific and explicit : silence does not imply consent. The Regulation clarifies the position of the data subject, the role and responsibilities of the data controller, and of the data protection supervisory authorities. The Regulation is not perfect, as Peter Hustinx acknowledged. Nor is it a panacea. But it is a significant step in the right direction.

Conclusions

The major innovation in the Regulation covers the international scope of EU law. Currently, which law is applicable depends on the locus of the responsible data controller wherever data is processed. Under the Regulation, the law will be uniform in all member states and any services offered to the EU market will have to comply with EU law regardless of the location of the provider. This also means that compliance with EU law will follow the data... into the cloud – even more than today.



Stronger, clearer and predictable accountability is intended to show users that they have more control over their data, and so to help boost trust in data handlers and trust in the credibility of legislation designed to enable them to enforce their rights.

The incentives for data handlers to comply lie in the costs of not doing so, including very large fines of up to 2% of gross annual turnover.

The Regulation is above all about uniformity and consistency in responsible data handling. Globalisation is no excuse for non-observance of EU principles and laws. It is likely to enter into force within the next two to three years following the completion of the co-decision process, complete with the usual wrangling over details in the Council of Ministers and the European Parliament.

Prof Dr Juliet Lodge
University of Leeds (UK)

EC answers to critical questions Sophie In't Veld and Sarah Ludford (MEP's) on performance of Dutch biometric passport

Regulation (EC) No 444/2009 of 28 May 2009 on biometrics in passports prescribes that passports and travel documents shall include a facial image and two fingerprints. Children under the age of 12 and people in whose case fingerprinting is physically impossible are exempted from this obligation.

During a hearing in the Dutch Parliament in April 2011 on the Dutch law on passports, reference was made to a test by the local government of Roermond. This test revealed that in 21 % of 448 cases, the fingerprints taken were non-verifiable and therefore useless. Based on this information MEP's **Sophie In't Veld and Sarah Ludford** has posed the following questions to commissioner Malmström:

- 1. Does the Commission consider that the Netherlands is in compliance with the requirements for quality and common standards for fingerprints set out in Council Regulation (EC) No 2252/2004?*
- 2. Will the Commission ask the Netherlands for an explanation of this high percentage of non-verifiable fingerprints, and of its inability to meet the requirements for quality and common standards for fingerprints?*
- 3. Will the Commission consider investigating the quality and verifiability of fingerprints in other EU Member States? Will the Commission inform the European Parliament of the outcome of this investigation?*
- 4. What added value does the Commission see for the inclusion of fingerprints in passports when 21 % of the prints are non-verifiable? Is the Commission considering re-evaluating the rules, given that these quality problems also appear to exist in other EU Member States?*

On 29th March, 2012, Commissioner Malmström has answered as follows:

"Since the implementation of fingerprints in passports in June 2009 no major problems have been reported to the European Commission related to recording good quality fingerprints in most cases. However, being aware of some quality issues, the European Commission continues to work together with the Member States to improve the situation. As a first step, the Commission adopted on 4 August 2011 a decision (C (2011) 5499) amending the technical specifications, further clarifying quality aspects and introducing a quality score for fingerprints stored in the chip."

"The Commission, in its role as guardian of the Treaty, undertakes tests of Member States' passports on their conformity with Regulation (EC) No 2252/2004 and the relevant technical specifications. While compliance testing is a standard procedure and is currently carried out by national accredited laboratories, the Commission's Joint Research Center (JRC) has performed and already reported on additional testing on the chips of electronic passports provided on a voluntary basis by some Member States to the Commission. Further reports will be issued in May 2012, including a report on the conformity of Dutch sample passports received. If non-conformity is found, the Commission will take the appropriate measures."

It remains interesting to see how the impact of the quality issues is being assessed and what the criteria will be used in order to come to a conclusion on conformity of the quality of the biometric data. We are also looking forward to learn more about the details of the cooperation between the commission and the member states to improve the situation, as the former BIG has been dissolved. To read the original Q&A between the parliament and the commission please go to:

<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2012-001306+0+DOC+XML+Vo//EN&language=EN>

French Constitutional Court rules against central storage of citizens' fingerprints

On March 22nd, 2012, the French Constitutional Court has ruled against several articles of the law for the protection of the identity of the French citizens. The most compelling decision is that Articles 5 and 10 have been skipped because they were considered to be a serious infringement of the French national constitution. In short this implies that the central storage of biometric data, as well as the use of these data for detection and prosecution purposes has been judged as being un-proportional and therefore against the constitution.

The Council has 10 objections to the way the scope of a law supposedly concerned with identity fraud and the protection of identity has moved into terrorism and many other areas. Three additional objections to the use of the proposed biometric ID cards for eCommerce were posed. These 13 counts of unconstitutionality are laid out in the [Commentary](#) which accompanies the decision and have been summarized in the Council's [press release](#), in which the law is judged to be disproportionate and to infringe people's right to privacy.

Article 5 of the act foresees into the creation of a database containing those data needed to apply for a French passport and national id-card. These data consist of state of marriage, place of residence, length, colour of the eyes, two fingerprints and a facial image. Article 10 provides the police and the national gendarmerie access to the database with personal information in order to detect and prosecute criminal offences, especially but not limited to terrorism.

The Constitutional Court has judged that the establishment of a central repository of personal data needed to issue identity and travel documents is needed in order to guarantee that issuance of these documents is safe and secure, and that such a database will increase the efficacy of fraud prevention efforts. So for these purposes it considers the central repository as justified based on common interest.

On the other hand, the Constitutional Court has researched the whole picture of the personal data contained by this administration, which has the purpose of collecting the personal information of almost the whole French population. Of all the collected information the fingerprints are the most sensitive. The technical properties obviously allow consultation for other purposes that just the verification of a persons' identity (1:1). It also allows to be consulted for police and judicial purposes.

With regard to the nature of the registered information, the size of the database, the technical properties and conditions which enable consultation of the stored information, the French Constitutional Court has judged that Article 5 is an unjustified infringement, as it is not proportionate to the initial purpose. For this reason the court has skipped Articles 5 and 10, as well as relevant parts of Articles 6, 7 and 8.

To read the official documentation please go to:

www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2012/2012-652-dc/communiquede-105166.html

In 2009 the Dutch Data Protection Authority (CBP, www.cbp.nl) came to similar conclusions regarding the Dutch passport act. Although the Dutch government ignored this opinion at first, it took several lawsuits and a drastic change of view with a majority of the Dutch parliament to make also this law to be turned down regarding the central storage of the fingerprint data.

3. EU Projects

BEAT: Europe to invest in biometric testing and evaluation

On March 1, 2012, the **Biometrics Evaluation And Testing (BEAT)** project, funded by the European Commission under the Seventh Framework Programme (FP7) and coordinated by the Idiap research institute has started., **Dr Sébastien Marcel**, principal Investigator of the project, is the Project Coordinator. The goal of BEAT is to propose a framework of standard operational evaluations for biometric technologies. This will be achieved by (1) developing an online and open platform to transparently and independently evaluate biometric systems against validated benchmarks, (2) designing protocols and tools for vulnerability analysis, and (3) developing standardization documents for Common Criteria evaluations. Additionally, legal aspects will be considered to address the issues of both privacy data protection and Intellectual Property and so ensure that the BEAT framework can be used by the research community and companies. Coordinator Sébastien Marcel:

"BEAT is of strategic importance to the fundamental enforcement of the biometrics and id- industry. European testing, evaluation and accreditation capabilities are essential in order to push biometrics as a technology further towards the reliability and trustworthiness which is needed to support current and future large scale deployments."

There will be three outcomes of this project. The first is that the reliability of biometric systems will be measurable and thus should lead to a meaningful increase in performance. The second is that technology transfer from research to companies will be much easier as there will be an interoperable framework. Finally, decision-makers and authorities will be informed about the progress that is made in biometrics as the results will have an impact on standards. Given these outcomes we expect that BEAT will significantly contribute to the development of a European Identification Certification System.

Raul Sanchez-Reillo, chair of the Testing and Evaluation Committee of the European Association for Biometrics (EAB) says about BEAT:

"The EAB strongly welcomes BEAT, as it will support existing testing and evaluation capabilities in Europe to get better aligned and test methods and the interpretation of the various test results. The EAB will seek to support BEAT within its scope of capabilities."

Please consult the project website for more information: <http://www.beat-eu.org/>

Fidelity: addressing shortcomings and vulnerabilities in the ePassport life cycle in Europe

Significant efforts have been invested to strengthen border ID checks with biometrics Travel Documents embedding electronic chips (ePassport). However, problems appeared regarding fraud in the ePassport issuing process, citizen losing control on their personal data, difficulties in certificates management, and shortcomings in convenience, speed, and efficiency of ID checks, including the access to various remote data bases.

FIDELITY is a multi-disciplinary initiative which will analyse shortcomings and vulnerabilities in the whole ePassports life cycle and develop technical solutions and recommendations to overcome them. FIDELITY will demonstrate privacy enhanced solutions to:

- secure issuing processes: authentication of documents, preventing impersonation fraud
- improve ePassport security and usability: authentication processes, ID check speed, accuracy of biometrics, management of certificates, access to remote data bases, convenience of biometric sensors and inspection devices
- better manage lost and stolen passports
- strengthen privacy: privacy-by-design applied to all phases of the ePassport life cycle, systematic anomysation of data and separation of data streams, using novel privacy-enhancing-technologies

FIDELITY will strengthen trust and confidence of stakeholders and citizens in ePassports, provide more reliable ID checks, hence hinder criminal movements, and ease implementation of E/E records providing better analysis of migration flows.

FIDELITY solutions will be designed for backwards compatibility to be deployed progressively in the existing infrastructure. The FIDELITY consortium is composed of market-leading companies, innovative SME, renowned academia, ethical-sociological-legal experts, and end-users, which will help to define requirements and recommendations and assess results. They will, with the other partners actively promote the project results towards stakeholders and international working groups that elaborate future ePassport standards.'

In case you would have any questions or need additional information, please do not hesitate to contact fidelity-arttic@eurtd.com



4. Academia

International cooperation: Carlos III University (Madrid) and the Purdue University (US) to develop BioAPI reference platforms

After the complete definition of BioAPI 2.0, standardized under ISO/IEC 19784-1, Purdue University (www.bspalabs.org, USA) and Carlos III University of Madrid (www.guti.uc3m.es/, Spain) have been working in developing open source reference implementations of BioAPI 2.0 in object oriented languages. Purdue University has developed a reference implementation in Java, available in www.bioapijava.sourceforge.net/. Carlos III University of Madrid has developed a reference implementation in C# for .NET based developments. This is available under LGPL licence at www.joinup.ec.europa.eu/software/bioapicsharp/home, to be included into any product, either open source or proprietary.

All members of the Biometrics community are invited to participate in the use and improvement of these two platforms, providing all desired feedback using the tools available at the two open source forges mentioned above.

Both institutions have offered this work to build the new multipart standard ISO/IEC 30106 (currently under drafting process). Comments and contributions to this work can also be sent via the National Standardization Body of each developer willing to contribute.

For more information you can contact Raul Sanchez-Reillo at raul.sanchezreillo@gmail.com.

5. Industry & Projects

WCC chosen to power a traveler management system for the Ministry of Interior of the Republic of Estonia

Given the volume of travelers, finite resources and limited time available for passenger processing, border agencies face significant challenges in identifying potentially risky travelers without delaying legitimate travel and trade. Using WCC's ELISE ID technology, Border officials can perform watch list checks for rapid risk assessment of passengers entering Estonia via flights from outside the Schengen region.

Processing international travelers for immigration and other purposes is a complex risk-sorting function. The vast majority of international travel is lawfully conducted, but some travelers present risks for security, illegal immigration, narcotics smuggling and customs revenue evasion. The combination of identifying risks earlier in the travel cycle and performing more

effective primary inspections improves the processing time for arriving flights and facilitates international travel.

The collection of pre-departure electronic data on travelers is emerging as the foundation of modern immigration control and border management. This approach is beneficial because electronic travel records can facilitate the implementation of a variety of automated functions, including watch list checks and risk analysis, before passengers arrive.

WCC Smart Search & Match has been integrated into Raytheon's Portera system to pilot a traveler management system for the Ministry of Interior of the Republic of Estonia that will facilitate more efficient processing of airline passengers. WCC's ELISE ID is used to pilot an automated risk assessment system that processes both Advance Passenger Information (API) and Passenger Name Record (PNR) data against a set of pre-determined risk criteria. WCC is providing technical support to the Republic of Estonia throughout the pilot.

36 e-passport based ABC gates started at Schiphol Airport

On 27th March 2012, Minister for Immigration, Integration and Asylum Policy Gerd Leers launched a trial scheme for an automated border control system at Schiphol airport. Using electronic gates equipped with facial recognition, passengers' identity is compared with the digital photographs in their passports. The system can also identify forged passports and wanted persons.



Dutch Minister Leers to kick off NoQ

These electronic border-crossing gates are intended to make passport controls faster and easier, while safeguarding security. The number of passengers passing through Schiphol is set to rise in the coming years, but there is a limit to the number of passport control desks or border police officers the airport can accommodate. The automated system will therefore take over some of the routine work of the Royal Military and Border Police, giving them more time to observe passengers. Officers will monitor the gates from a distance and can always decide to carry out further checks on a passenger, if necessary. The electronic gates are intended for passengers with biometric passports issued in EU member states or in Norway, Iceland,



Liechtenstein or Switzerland. In the next few months, passengers will be invited to use the electronic gates. The aim is for the system to be fully operational next year. A total of 36 gates will be installed (in departure hall 2, arrivals hall 3 and the Schengen/non-Schengen border crossing area). Passengers will still have the option of using the passport control desks. The Ministry of the Interior and Kingdom Relations, the Royal Military and Border Police and the Schiphol Group are responsible for this project. The system was developed by Accenture, and will be produced in collaboration with VisionBox.

Source: Dutch Ministry of the Interior

German Border Police chooses secunet for the DVCA project

secunet won the German Federal Police's tender to establish the central certification authority for national border posts. The so-called DVCA (Document Verifying Certification Authority) provides central certificates that are necessary to check electronic identity documents at national border control posts. The data saved electronically in current identity documents, such as the new German ID card (nPA), are protected against unauthorized access by technical measures. In order to access data at checkpoints, the reading devices used by border officials must be equipped with the digital certificates issued by the Federal Police. secunet was commissioned to set up the required DVCA to generate these certificates. The certificates generated by the DVCA are transmitted to the Terminal Control Center (TCC). The TCC performs the cryptographic functions and key management for the connected border control posts and the partially automated EasyPASS border control at Frankfurt airport. secunet already implemented the Terminal Control Center on behalf of the German Federal Office for Information Security and developed a border control application to read electronic identity documents at the German border. secunet developed and implemented essential parts of the German border control infrastructure for electronic identity documents. Background information

Today's identity documents are protected against unauthorized access by the Extended Access Control (EAC) mechanism. This mechanism is based on a three level public key infrastructure. The actual reading instance (inspection system/IS) gets a digital certificate from the corresponding organizational unit responsible for the document verification (e.g. the border police). The document verifier (DV) itself is entitled by the appropriate country verifying certification authority (CVCA). This certificate chain is used by the terminal during the verification process to authenticate itself to the document as a legitimated instance.

Opportunities for biometrics in the mobile market

Mobile technology has advanced quickly and created all-rounder which accompany and support us in our day-to-day life. They yield many possibilities of applications, but are also associated with high risks. Who can guarantee that the user of a phone or tablet is actually allowed to use



all the mobile services? To solve this security problem **BIOMETRY.com AG** has developed the product MobiComBiom (Mobile Communication Biometrics). This guarantees unique user authentication by requesting four authentication processes – biometric face recognition, biometric voice recognition, recognition of biometric lip movement, and word recognition – simultaneously with randomly generated numerals through random challenge response or otp (one-time password). By pressing a specific “soft button” on the cell phone (e.g., numerals 1 and 3 are pressed simultaneously), the MobiComBiom authentication process is started. With it, four randomly selected numerals appear successively on the cell phone display. Similar to video telephony, the user speaks these numerals. The video and audio data is then securely transmitted to the provider where every numeral is converted into files. These are compared to the reference data that was previously learned by the user for the numerals 0,1,2, to 9. If the data matches, the user of the cell phone is uniquely authenticated. For more information please visit www.biometrivy.com.

European Biometrics Group to conduct a study for the European Parliament on the e-passport in Europe

The European Biometrics Group (EBG) has been assigned by the European Parliament to conduct a study on the implementation of EC22025/2004 by the EU member states. Focus will be on the capturing, management and storage of the biometric data, including aspects such as quality assurance, legislation, public perception, use cases and interoperability. More information: m.snijder@eubiometricsgroup.eu.

6. Outside Europe

NIST publishes IREX III results

IREX III, the third activity in NIST’s Iris Exchange (IREX) quantitative standardization program, was the first public, open and independent evaluation of the capabilities of one-to-many iris identification algorithms. By applying implementations, from academia and industry, to a database of 6.1M images of 4.3M eyes of 2.2M people, the study was aimed at adding further numerical support to the long standing claim that iris can uniquely identify individuals very quickly. Conducted in two phases spanning a 7 month period in 2011, IREX III evaluated 95 algorithms from 11 developers against criteria including accuracy (false negative + false positive identification rates), resource usage (template size, memory, speed) and sensitivity to various parameters (compression, dilation, iris size). The reports from IREX III are available here: www.nist.gov/itl/iad/ig/irexiii.cfm.

7. Events

IBPC 2012 Conference report

The second International Biometrics Performance Conference (IBPC 2012) and its three satellite workshops took place at NIST (Gaithersburg, USA) from March 5 – 9, 2012. More than 160 participants from governmental agencies, industry and academia (including 45 speakers from 11 countries on 4 continents, including representatives of 6 governments) convened to discuss topics related to performance and conformance testing of biometric components and systems. Slides from the conference are available at: www.nist.gov/itl/iad/ig/ibpc2012_presentations.cfm

Highlights of the conference were report about the evaluation of large scale biometrics systems both a technology tests (**Patrick Grother** reporting about IREX III and MBE) as well as scenario / operational testing (**Raj Mashruwala** and **Srikanth Nadhamuni** on the Indian UID system). While ground truth composition and sanitization for biometric testing was a topic covered in various presentations the talk by Brad Ulery on accuracy and reliability of latent fingerprint examiners caused specific attention as it might be cited in court when it comes to assessment of forensic investigations. The conference also presented and discussed the preliminary results of the **NFIQ2.0** project and the candidate quality features that are under consideration for the NFIQ2.0 quality metric. For more more details see: www.nist.gov/itl/iad/ig/development_nfiq_2.cfm

A further dominant topic of the conference was mechanisms and standards for artefact, liveness and Suspicious Presentation Detection (SPD) techniques - commonly known as spoof detection. The discussions around this topic compose content that is a relevant input to the current ISO/IEC 30107 standardization project. The next IBPC will take place in 2014.

IBC 2012 Conference Report

From March 29 to April 1 the 5th IAPR International Conference on Biometrics (ICB 2012) took place in New Dehli, India. The rich program included scientific research results on all biometric modalities. An impressive Keynote by **Nandan Nilekani** was presenting the Biometric and inclusion concept that is providing each Indian citizen an identity. A further notable keynote by **John Daugman** outline the 20 years experience from his first IEEE Pami publication until today. The best research paper award was given to **Oleg V. Komogortsev** (Texas State University), **Alex Karpov** (Texas State University), **Larry R. Price** (Texas State University), and **Cecilia Aragon** (University of Washington) for their paper Biometric Authentication via Oculomotor Plant Characteristics.

Information on the further awards and the program of the conference is available at: www.icb12.iiitd.ac.in/index.html



EAB workshop "Transcontinental Perspectives on Privacy and Metrics for Biometric Template Protection" in cooperation with NIST and BI: Paris, Friday 13th July, 2012

The EAB is organizing a workshop **"Transcontinental Perspectives on Privacy and Metrics for Biometric Template Protection"**. The event will take place in Paris on Friday, 13 July, 2012, and is co-located with ISO/IEC JTC1 SC37.

The workshop will be organized in cooperation with the National Institute of Standards and Technology (NIST) and the Biometrics Institute (BI). The objective of the workshop is to analyse commonalities and differences of the various continental privacy cultures with regards to processing of biometric references and privacy impact assessment (PIA) and to present technical concepts for Biometric Information Protection. A core element of the workshop will be to discuss metrics for benchmarking of Template Protection Algorithms and to identify in the communication between industry and academia, if suggested metrics serve industry needs. This workshop will prepare the next step needed for wider deployment of Biometric Template Protection, which is a standard to assess and evaluate such techniques. For more details see:

http://eab.org/events/upcoming_events.html or contact the EAB secretariat at secretariat@eab.org

Security Document World 2012: London, 21-23 May, 2012

On 21-23 May, 2012, the Security Document World (SDW) conference and Exhibition will take place in the Queen Elizabeth II Conference Centre in London. SDW 2012 is the 'number one' international event for technology suppliers, security document printers, infrastructure providers and integrators in the fast-moving security document market place. For more information and book your access card please visit www.sdw2012.com.

BIOSIG 2012 conference: Darmstadt 6-7 September, 2012

Nowadays, biometric applications are growing rapidly and have reached different areas such as health monitoring, national ID cards, e-banking, e-commerce, etc. The European Union Visa Information System (VIS) and the Indian UIDAI System are large-scale deployed systems that validate the capabilities of today's biometric products. However deployed systems are still facing challenges towards better biometric performance, interoperability, system reliability and usability.

New modalities and innovative acquisition techniques such as efficient 3D-face reconstruction taken from a distance, multi-spectral fingerprint images, in vivo imaging are important to increase the versatility of biometrics and its area of use. Moreover biometric recognition is now used as access control schemes towards mobile phones with its embedded sensors such that many convenience applications can now be served. Both in security and convenience applications efficient fusion techniques for multimodality systems are necessary to improve performance and robustness. When biometrics is chosen to increase the security of an access control system then the security of the



EAB Newsletter, edition April 2012

biometric system itself must be investigated. This includes fake resistance of sensors, biometric information protection and crypto-biometrics to enhance the privacy of data subjects and to protect biometric references. Moreover, security analysis and certification of security properties need to be developed. Beyond that critical issues such as the compliance to standards and the early assessment of sample quality with standardized metrics systems are important to guarantee successful use of biometrics in practice.

The BIOSIG 2012 conference addresses these issues and will present innovations and best practices that can be transferred into future applications. The conference is jointly organized by:

- the Competence Center for Applied Security Technology (CAST)
- the German Federal Office for Information Security (BSI)
- the European Association for Biometrics (EAB)
- the Joint Research Centre of the European Commission (JRC)
- the TeleTrusT-Association, the Norwegian Biometrics Laboratory (NBL)
- the Center for Advanced Security Research Darmstadt (CASED)
- the Fraunhofer Institute for Computer Graphics Research IGD
- the special interest group BIOSIG of the Gesellschaft für Informatik e.V. (GI).

The call for papers for BIOSIG 2012 is available at: <http://www.biosig.org/biosig2012>

World eID Conference: Nice, 17-21 September 2012

On 17-21 September the World eID conference will take place in Nice as part of the 'World Smart Week'. The World Smart Week consists of 3 events:

- NFC World Congress
- World e-ID Congress
- Chip-to-Cloud Security Forum

The location is at the Acropolis Convention Center of Nice. Acropolis is located in the center of Nice city, only 15 minutes from the Nice International Airport & 700 meters from "Promenade des Anglais" and seaside. The total audience of the 3 conferences from Sept 17 to 21 will be of 1500 delegates from 75 countries, including about 80 press and media editors and journalists. Many "add-ons" will be proposed to the delegates such as: workshops and trainings, research labs visits and demos, live experience of NFC and Identity services, proprietary presentations, press conferences and announcements, social events and cocktails...

The joint exhibition will be open from Sept 18 to 20. At least 2500 visitors (in free access) will have the opportunity to discover its 70 booths and 150 demos and innovative solutions covering the whole contactless and identity solutions domain.

Being an EAB member you will receive a special rate with a 30% reduction. Please contact Lenick Peron for more information or to reserve your ticket to the event:

lperron@strategieism.com. You can also visit the website at www.worldsmartweek.com.



EAB Newsletter, edition April 2012

Colofon

Publisher: European Association for Biometrics

Editors: Georg Hasse / Max Snijder

Production: European Biometrics Group

Contact: secretariat@eab.org / georg.hasse@secunet.com

Phone: +31624603809

www.eab.org