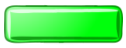
Roadmap for biometrics

Description and state of the art	
Definition	*Biometrics* as a characteristic is a measurable biological and behavioural characteristic that can be used for automated recognition and as a process it encompasses automated methods of recognizing an individual based on measurable biological and behavioural characteristics[107]. Biometric identifiers are often categorized as physiological and behavioural characteristics, where the former are related to the shape of the body (fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odour/scent, etc.), while the latter are related to the pattern of behaviour of a person (e.g. typing rhythm, gait, voice, etc.). Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control[108]. Biometric authentication methods use biometric characteristics or traits to verify users' claimed identities when users access endpoint devices, networks, networked applications or Web applications[109].
Addressed societal /business or public sector need	Societal need: Faster and transparent access to public sector services
Existing solutions /applications /services	Biometrics has found several application in the public sector, e.g. in border control, visa programs as well as in government and law enforcement agencies, for example: • **Automated e-Passport gates** -- self-service kiosks that verify a traveller's identity with biometric recognition software[110] • the Australian **Tax Office** (ATO) is an example of a leading public sector organisation that has already embraced voice biometric technology[111] • In **Belgium**, citizens use their ID cards to manage their social security, request car licence plates and conduct their tax declarations over the internet. [112]

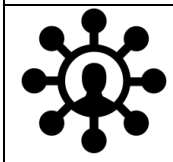
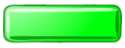
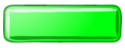
	Biometric visa program: With the exception of France, which had already implemented biometrics in its visa program, the **European Union** and **Schengen Treaty countries** began rolling out their biometric (fingerprint and digital photograph) visa program in October 2011. *Biometric identity cards (e.g.):* **Bulgaria** began issuing biometric identity cards (mandatory for all citizens) in March 2010. Bulgaria also issues biometric passports and driver's licenses containing embedded biometric data.[113] **Finland** introduced biometric residence permit cards in 2012. The cards include a chip that stores a digital photograph and two fingerprints.[113] **France** has issued only biometric passports since 2009. The passport requires the collection of a biometric digital photo and eight fingerprints.[113] In May 2005 the **German** Parliament already approved the implementation of the ePass. The ePass has been in circulation since November 2005, and contains a chip that holds a digital photograph and one fingerprint from each hand.[114] In accordance with EU standards **Luxembourg** issues biometric passports with a chip containing a digital photograph, two fingerprints and an image of the holder's signature.[113] Since 2009 the N**etherlands** has issued biometric passports containing an embedded chip with a digital photograph and fingerprints. Although only two fingerprints are stored on the passport's chip, four fingerprints are taken and stored by the local government in a central database that is also used to pursue criminal investigations.[113] In **India**, the government-led national identity program Aadhaar aims to establish a biometrics-based registry for all 1.2 billion of its residents. After having their identity verified, registrants receive a unique 12-digit ID number that allows them to access a range of government and private sector services. Aadhaar is the most ambitious government-led biometrics program in the world, with over 900 million Indian residents already enrolled.[110]

 Main actors regarding R&D of this technology	• Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung e.V • Morpho • Katholieke Universiteit Leuven • Centre National de la Recherche Scientifique
 Current research activities	**FP7-projects:** 4DVIDEO, ACTIBIO, ADABTS, ADDPRIV, AMASS, ANASID, BBFOR2, BIO, CAPER, CLOVISEN, COPRA, CRESCENDO, DEMASST, DETECTER, DIGIDEAS, DIGITAL.ME, EFFISEC, EGAIS, EIW3R, ELSAIDTCGT, ETHICAL, ETHICSWEB, ETICA, EU, EUCONRES, EUCRIMINALSECURITY, EURECNET, EUSECON, GEST, GINI, HBP, HIDE, ICTETHICS, IDETECT4ALL, IMSK, INDECT, INEX, LAST, MOBIO, MOSAIC, MUSIS, MUTIVIS, NORDIA, OPERAMAR, PASS, PATS, PERSEUS, PHM, PHM, PRACTIS, PRESCIENT, PRIMELIFE, PRISM, PROMETHEUS, RISE, RTD, SAMURAI, SAPIENT, SEARISE, SECTRONIC, SENIOR, , SEPIA, SEREN, SFLY, SMART, SMARTENC, SNAPS, SUBITO, TABULARASA, TACO, TALOS, TASS, TECHNOLIFE, TERATOP, TURBINE, VANAHEIM, VIDEOSENSE, VISION, VPH **Other EU-projects:** AMBER (mobile biometrics), PROTECT (automated border control), SpeechXRays (speech biometrics), BEAT(evaluation and testing), BIO-DISTANCE (biometrics at distance), BIO-RESIDENCE (access), BIOHEALTH (eHealth) **BMBF:**[3, 108] GES-3D, MARS, MisPel, FeGeb[109], CRISP, IP2 Projekt[110] B**SI**:[111] BioFace, BioFinger, BioP, BioKeyS, NFIQ2[112] **EUROSTARS projects**: MOBITOUCH-ID[113], BioSec[114], BioSpeak[115], BIRDS [116], ASSURE-ID[117]
 Impact assessment	**Public Sector Modernization**: • Efficiency / Productivity • Sustainability • Cross-organization cooperation • Quality of Services provided • Transparency • And negative impact on "creation of trust and confidence" **Public Sector as Innovation Driver:** • Public Safety • Transport Infrastructure • e-security • and negative impact on equity and inclusiveness as well

	as on privacy and security
Necessary technological modifications	
 Potential use cases	• Physical access control • Computer log-in • Welfare disbursement • International border crossing / Border management / Speed mobility in borders • Airport kiosks for checking passports • Driver's license • Facial recognition to speed up processes and manage queues • Identify criminals on the fly • Avoid fraud on competitive examinations • Life identification against watch lists (terrorism)
 Technological challenges	Most of the research in biometric recognition has focused on the following two fundamental problems:[115] • The challenge of identifying **the best feature representation scheme** for a given biometric trait (e.g. fingerprint, face and iris). The desired set of features should retain all the discriminative information that is distinctive to a person and remain invariant to intra-subject variations. • The challenge of **designing a robust matcher** (e.g. face or fingerprint matcher) for a given representation scheme. The desired matching algorithm must model the variations in the features belonging to the same individual, while accounting for variations between features of different individuals. The unsolved problems in biometric recognition can be divided into two categories: (i) problems that involve fundamental issues related to design of recognition systems and (ii) problems that are specific to applications that will use biometric recognition.[115] Feature extraction and matching schemes that can **handle poor quality biometric samples** (e.g. face images from a surveillance video or latent fingerprint images) need to further developed. In the case of application-specific problems, the two main unresolved issues are (i) techniques to **shield a biometric system** from adversarial attacks/threats and provide assurances on user privacy, and (ii) techniques to **assess usability of a biometric system** and estimate the return on investment. Other unresolved challenges are: [115] • **Distinctiveness of biometric traits** (estimating the individuality of a biometric trait) • **Persistence of biometric traits** (Persistence of a biometric trait is related to the notion of aging. Aging refers to changes in a biometric trait or the

		corresponding template over a time span, which can potentially impact the accuracy of a biometric system) • **Unconstrained biometric sensing environment** (There are some person recognition applications where it is very difficult to impose constraints on how the biometric trait should be acquired. One example is latent fingerprints acquired from crime scenes.) • **System security and user privacy** (the biometric system may be vulnerable to a number of security threats, which may eventually affect the security of the end application)
Necessary activities (in or for the public sector)		
 Development of a specific training necessary		For the actual usage of biometric identity systems no training is needed. The selection and implementation of these systems has to be done by experts.
 Advanced or adapted ICT infrastructure needed	**Open task**	Yes, specific hardware like a sensor, biometric processor and template storage is needed.
 Change of (public sector internal) processes necessary	**Open task**	Yes, the public sector processes (like authorization processes to online services) have to be adapted to the usage of biometric identity systems.
 Promotion / information of stakeholders necessary		No issues identified in this area.
 Need to deal with cyber security	**Open task**	Recent "breaches of security", including the Snowden incident, have made the public increasingly sceptical about who has access to their biometric data and whether it is stored securely. Research Councils UK stated that establishing public confidence in "the storage

issues		and access arrangements around their biometric data" was key to ensuring greater public acceptance of biometrics[116]
 New or modified legislative framework or regulations necessary		There are a number of data protection issues associated with the storage of personal (biometric) data. In particular, the ensured accuracy, security, control and proportionality of that storage are especially important.[117] However, on May 25, 2016 the EU Data Protection Regulation came into force. The new legislation, which was several years in the making, encompasses all recent technological developments including biometrics.[118]
 Development of a common standard necessary		Several national and international players are developing biometric standards. They include the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and ITU's Telecommunication Standardization Sector (ITU–T). Industry consortia also develop standards that support the objectives of their membership, while United Nations specialized agencies, such as the International Civil Aviation Organization (ICAO) and the International Labour Organization (ILO), develop standards within their specific domains that might not have been addressed by other organizations. In particular, ICAO is responsible for the standardization of machine-readable travel documents, including electronic passports, while ILO has provided guidelines on biometric identity documents for seafarers.[119]
 Need for a more economical solution		This depends on the specific application and the country, e.g. the national biometric passports vary in their price depending on the country of origin.
 Ethical issues	**Open task**	The application of biometric data and technologies raises ethical and legal questions related **to privacy, autonomy, informed consent, confidentiality and liberty**.[116] By turning the human subject into a collection of biometric parameters, biometrics could dehumanize the person,[120] infringe **bodily**

		integrity, and, ultimately, offend human dignity.[121] There are three categories of privacy concerns:[122] • **Unintended functional scope**: The authentication goes further than authentication. • **Unintended application scope**: The authentication process correctly identifies the subject when the subject did not wish to be identified. • **Covert identification**: The subject is identified without seeking identification or authentication, i.e. a subject's face is identified in a crowd. One of the major concerns aired by opponents of biometrics technologies is that they pose a threat to individual privacy. But advocates argue the opposite, that biometrics can be used to safeguard citizens against data breaches, identity theft, fraud and other violations of personal rights.[110]
 Societal issues		No societal issues identified.
 Health issues		No health issues identified.
 Public acceptance	**Open task**	According to Sir John Adye, Identity Assurance Systems, public distrust of biometrics remained "prevalent in countries like the UK" while Professor van Zoonen, IMPRINTS, identified biometrics as "the most controversial and worrying of all means of authentication" among the British public[116]