Thomas Petermann
Constanze Scherz
Arnold Sauter

December 2003

TAB

Biometrics and identity documents Performance, political context, legal considerations

Summary

TAB Working report no. 93

TAB
Office of Technology Assessment
at the German Bundestag

SUMMARY

CONTEXT AND OBJECTIVE OF THE REPORT

A global breakthrough by biometrics in security technology seems to be imminent in the form of its use in identity documents and corresponding biometrically-based controls at frontiers. All over the world, states and groups of states are creating the political and legal conditions for this.

The question of which biometric systems and which features are suitable or preferable is now much less open than it was only recently. Recognition systems using fingers, faces or irises (or a combination of these features) have, in principle, proved their suitability for applications verifying identity documents, although their performance and capability could be improved in some respects, depending on the context and system requirements. However, one significant dilemma remains for decision-making: the biometric enhancement of national ID documents and their global use in border controls constitute a task on such a scale that experience to date – e.g. with pilot projects on border controls – can, at best, provide only indirect information. In view of the volume of international travel and migration and the complexity of the necessary technical, administrative and legal implementation at national level – and a fortiori on a global scale – our present state of knowledge and experience is still in a state of flux. At the same time, however, there is obvious need for action.

In this situation, an objective of the present TAB report on biometric identification systems is to present the current state of discussion. The report is not the result of a comprehensive technology assessment, as the review was limited in terms of the issues covered, and specifically there was no analysis of consequences. In accordance with the commission, it summarises the status of scientific and political discussion of the capability and suitability of these technologies and corresponding systems for specific identity documents and border control applications, formulates requirements for legally compatible design and addresses further need for information, discussion and action. The status report is accordingly intended to assist the work of the committees of the German Bundestag.

POLITICAL ACTIVITIES AND DECISIONS, INTERNATIONAL DEVELOPMENTS

In many countries, tests, pilot projects and feasibility studies – and increasingly legislation and regulations – have laid the foundation for biometric enhancement of identity documents and biometric border controls (section II). Many countries have already decided on national identity documents with biometry or taken the first steps (section III). The USA has for some time been moving towards a biometrically-supported system for border entry and exit controls. At EU level basic political and legal decisions have been taken, creating the conditions for coordinated use of biometry or biometric enhancement of identity documents, visas and residence permits for non-EU nationals. In Germany the Passport and Personal ID Act and the Aliens Act have been amended accordingly. Additional biometric information (face, finger, hand) can now be integrated into identity documents for German citizens and aliens. However, further operationalisation of modalities and details is required by the legislators and regulators.

The G8 nations constitute a further actor. They intend to create a high-level working group under joint US-French leadership to prepare the initial political decisions. Large-scale test programmes are being considered for preparation. The G8 nations explicitly support the International Civil Aviation Organisation (ICAO) and its efforts to standardise biometric procedures.

After long preparatory work, the ICAO (a United Nations specialised agency) has issued a recommendation on making inclusion of a facial picture in international travel documents, as the first physical characteristic, binding on member states. Fingerprints and/or iris images are given as options for nations wishing to use biometry for checking with databases.

TECHNICAL PERFORMANCE AND SUITABILITY

The report summarises the state of discussion on the technical performance and suitability of hand geometry, fingerprint and face and iris recognition for use with identity documents and for verification at border controls. For this purpose, a short general description of the strengths and weaknesses of the individual biometric procedures (section IV.1) is followed by a more detailed description of their specific performance profile for identification use (section IV.2).

A review using various criteria reveals the following situation:

- If IDs are biometrically enhanced, care must be taken to ensure that the proposed feature as far as possible excludes nobody or a very small number of citizens from the application. Fingerprint procedures only partly meet this criterion. Tests and experience to date show that problems arise with biometric enrolment with around 2% of the total population. While the enrolment failure rate is lower with hand and iris recognition processes than with fingerprints, there are still problems with certain user groups due to their age or ethnic background. The user failure rate for facial recognition is marginal.
- Hand geometry recognition is relatively less suitable with regard to the requirement of discrimination, particularly with extensive application. Discrimination is fundamentally better with iris, finger and face, because of the large number of unambiguous pieces of information. Solid quality tests demonstrate the high degree of uniqueness of the finger and face as features, even with large data populations. There is no evidence yet from large-scale applications for the iris.
- For biometric applications, it is important that a feature should not change over a short period of time. In terms of stability, the fingerprint process is open to criticism because of certain limitations. A drawback with hand geometry recognition is that this feature only stabilises late, at the age of 20. The stability of the face is sufficient for identification use, as changes in this occur over longer periods, so that »reregistration« can be done at reasonable input/cost. The iris probably has least problems with regard to the criterion of stability.
- Studies to date suggest a high recognition performance for iris recognition processes, although this has yet to be checked in large-scale applications. While hand geometry recognition showed good recognition rates in small-scale situations, the problem of the ambiguity in discriminating between hand geometry samples in larger-scale applications would need to be settled in large-scale test studies. Fingerprint and face recognition processes have demonstrated their recognition performance in current and independent studies, even for large data sets. The current performance level of the two processes in verification applications is roughly equal. Both fingerprint and face recognition processes today are sufficiently mature and have sufficient performance capability for their use in verification mode to represent an increase in the effectiveness of border controls, compared with the present situation. The question whether the recognition performance to be expected here will ensure adequate security, and whether the anticipated improvement in border controls justifies the expense involved, is one which requires political justification and decision. A point for open debate here is that despite impressively low error rates, mass use in practice can only result in a relative increase in security, as misidentifications will continue to a certain extent.

> For identification use, processes with low operating cost and high comprehensibility are advantageous. Face recognition processes have advantages here as a contactless process without major positioning effort. Fingerprint processes are convenient in use, but require a learning period, although this is only short. Operating errors are also relatively rare in hand geometry recognition. Iris recognition is comparatively less favourable in terms of the effort involved in operation, as it requires exact procedures and some learning time. The effort with enrolment and control required with all processes should not make any decisive difference in the current time frame for application for an ID and control processes. However, a comprehensive assessment requires consideration of further aspects, such as the system environment and structural, infrastructural and organisational aspects. Whether – for example – more time would be required at the airport for ID controls, or whether biometric procedures could result in saving time in the longer term depends on the specific system conditions and local service requirements.

Each technology has specific strengths and weaknesses. For example, face recognition leads on two criteria (enrolment failure rate, operating effort and comprehensibility), but falls behind on recognition performance. Iris recognition leads in terms of recognition performance. However, it lags when it comes to operating effort. Hand geometry recognition has average ratings throughout overall, but a high false positive (recognition) rate. Fingerprint recognition does not outperform any of the other processes in terms of any single criterion, but has good ratings on average, with the exception of the unsatisfactory enrolment failure rate.

Overall, we can conclude that three processes – face, iris and fingerprint recognition – have roughly comparable technical capability. By contrast, hand geometry is somewhat lacking. A decision for or against a specific technology requires consideration of further criteria and issues.

EFFECTS ON EXISTING PROCEDURES FOR DATA COLLECTION AND PRODUCTION

Implementing the goal of biometric modernisation of IDs and ID controls could have substantial consequences – for example, a complete collection of biometric data for German citizens. If we consider the consequences of various options for the limited area of the survey and production processes for passports and IDs, we find the following consequences (section IV.3):

Data collection

In terms of the organisational inputs, the most practicable option with the current ID concept and within the context of existing and familiar data collection and production processes would be to use photographs of adequate quality on the ID for automatic analysis. A template could be generated centrally or locally.

For fingerprint, hand geometry and iris recognition processes a complete collection of biometric data for the German population would be required. Decentralised data collection would require equipping all citizen and alien registration offices with biometric systems, and training staff in their use. In the case of central data collection, generating a template for a fingerprint would require an impression of the print. Trained staff would be needed to ensure adequate quality. Iris and hand geometry recognition require decentralised data collection at the registration offices, as the features cannot be filed as raw data and forwarded for processing.

While there is extensive experience from large-scale application with collecting fingerprints and face recognition, there is a lack of experience of large-scale data collection and maintenance for irises and hand geometry. Problems with the collection of iris and hand geometry data for the entire population should accordingly be carefully considered in advance.

Data storage on the document

The consequences of introducing and using biometry for the established document concept can be outlined as follows: There would not be major consequences of storing faces in optical form by printing a photo on the ID, as this process is already an established part of ID production. If biometric analysis of the face could be based on the photo, there would be no need to store a biometric template. For this, it would be necessary to ensure an adequate standard (e.g. ICAO). Storing the photo of the fingerprint requires modification to the ID, as the photo would have to be stored in addition to the facial photo. There is, however, no provision for this on the current ID.

When integrating a biometric template into the ID using a barcode, a point to consider is that the barcode can only be applied during central production. There is currently no provision for storing the barcode on the ID.

Integrating a chip into the ID would involve considerably greater input/expense, among other reasons because of the lack of infrastructure (readers). Contactless chips could be integrated into the existing document, but not contact-based chips. An advantage is that the data can only be entered on the chips when the document is issued. Because of the lack of large-scale application and testing, no reliable statements can be made yet about security from manipulation and durability. Storage in chip form is the process requiring highest inputs because of the changes required in production, but it offers greater potential in application.

COSTS

The discussion of costs is still in its infancy. However, we can say that the various identification technologies involve hardware and software costs which are comparable in scale. We can further say that the biometry components are not the decisive cost factor in the overall system. As an initial step in answering the question of the total cost (nonrecurring and current) at all levels of the system, cost models are explored for various application scenarios (section IV.4).

> Biometric use of existing documents (option 1)
Here, the passport photos printed on the IDs with facial information on the individual are used for biometric analysis. The current application process together with providing a passport photo would be retained. The main modifications required would be at the level of issuing the document, with the need to standardise the quality of passport photos.

> Technical upgrade to existing documents with biometric data (option 2)
The data is applied to the ID using storage technology. Possible forms of storage are barcodes or digital storage components. Alternatives would be central entry and processing of biometric features (2a) and decentralised entry and processing of biometric features at the individual registration offices (2b).

> The existing document concept is replaced by a completely new one (option 3)
In this alternative, the document (e.g. smartcards) is enhanced by an electronic storage component. This would open up possibilities for combining the general use of electronic signatures and possibly be a stimulus for electronic commercial and legal transactions.

A rough estimate of nonrecurring and current annual costs shows the following picture:

Option 1 requires 22 million in nonrecurring costs and 4.5 million in current costs. Option 2 requires 614 million in nonrecurring costs and 322 million for the decentralised re-entry (variant 2b) and 179 million and 55 million respectively for centralised processing (alternative 2a). Option 3 as the most sophisticated technology requires nonrecurring investment of 669 million and 610 million in current annual costs.

The cost comparison also shows that options which require decentralised re-entry of features and template generation (involving new hardware) involve costs which are several times greater than those for alternatives where the extra expense arises in production of the IDs.

Despite its importance, cost alone is not a sufficient basis for a decision. Further aspects – in the sense of a cost-benefit analysis – would have to be considered. A provisional review suggests the following considerations:

Assuming that the increase in security is roughly the same for all alternatives, arguments in favour of option 1 (face recognition technology) are the low cost, the retention of existing processes, and likely greater acceptance among the population. A further consideration is that this option leaves open the possibility of moving to other options. Arguments against it are the conservative nature of the approach, which does not offer any stimulus to innovation or open up additional uses.

Option 2 involves higher costs and raises the issue of the acceptance of full-coverage enrolment of German citizens. Conversely, retaining the family of documents would maintain a certain continuity, and a higher level of technology would be attainable.

Option 3 combines the dimension of security with innovation policy prospects. Although it involves the highest costs, the introduction of a modern card would probably be an innovative approach which would also trigger economic impacts. For German citizens (and in the medium term for foreign nations resident in Germany) this would result in a document which not only allows conventional authentication but could also be used as the basis for electronic signature in electronic commerce.

LEGAL BASIS

The Act to Combat International Terrorism, which entered into force in January 2002, contains an important element in the regulation for the inclusion of biometric features in passports and IDs for Germans and IDs for foreigners. The

Act provides for the possibility of including features in addition to the photo and signature in passports and IDs, including in coded form. At the same time, new regulations are making possible the inclusion of such biometric features in IDs for foreigners and asylum-seekers. The nature of the biometric features, their details, the method of storage, other processing and use will be separately regulated in an implementing act or regulation yet to be promulgated. This expresses the intent of the legislature to improve the possibilities for computer-assisted identification of individuals based on IDs, among other things to prevent individuals using documents as identification which belong to people with similar appearance. The current legislative basis can be described as follows (section V):

- With respect to the IDs for German citizens, the law states that the biometric features may only be read and used to check the authenticity of the document and check identity, so that the principle of dedicated use derived from the constitutional right to self-determination with regard to information is adequately observed. The situation is very different in the case of »foreigner IDs”. Here, provision is made for recording biometric features, but there is a total absence of adequately defined purposes. Section 5 (7) of the Aliens Act contains a general authorisation for all agencies to process this data in the course of the legitimate functions. This cannot be reconciled with the constitutional requirements for dedicated use and specificity.
- The legislature has limited the biometric features concerned to »fingers or hands or faces”. This excludes not only other features, but also combinations of a number of features. In the current state of the technology, this restriction causes problems as it means that under some circumstances the full capability of biometric systems cannot be exploited.
- With respect to the selection of the permissible individual biometric features, it must be borne in mind that the use of biometric processes can result in additional sensitive and person-related information. This is why it is necessary to limit the risks associated with recording the biometric features. A primary candidate for this is avoiding storing raw data.
- The authorisation created by the legislature (without more detail) to integrate the features and data into the relevant document in coded form requires exact regulation of the question of how the coding is to be done or the biometric data are to be authenticated with an electronic signature. In view of the security environment required for this, central production of the documents seems preferable.
- Storage of the data in a central register is currently precluded by statute for German citizens. Storage on the ID would be sufficient to satisfy the purpose of the law. The creation of central reference files for aliens is not ruled out by law. However, central data storage by public agencies without strictly limited

uses poses problems because of the unequal treatment in the sense of section 3 of the Fundamental Law and the principle of proportionality. Decentralised storage of data in a register would, for example, make it possible to use this for criminal investigations or in a dragnet. Storage of biometric features in a database, access to which is not limited to the individual concerned, poses the risk of misuse and creating problems in terms of data protection.

Storage of biometric features of aliens would be acceptable in terms of the constitutional right of self-determination with regard to information, if storage outside the ID is at a decentralised or central alien agency, provided that there was statutory limitation to data security purposes.

NEED FOR FURTHER INFORMATION, DEBATE AND DECISION

At the level of legislation and regulations, clarification is needed of important aspects of implementing legislative regulations to date. The preliminary decisions by legislators will probably require new discussion. Here, for example, the situation has to be considered that the use of biometric data in regulating residence rights has so far not been specified. Well-defined use would largely resolve data protection concerns, and make the goals of legislation and regulations largely transparent.

A further point to be resolved would be whether the limitations of the biometric features involved to »fingers, hands or faces« would continue in future, or whether legislation should open up the possibility of a combination of a number of features or systems. This could under certain circumstances permit better utilisation of the performance capability of biometric systems.

Given the desirability of protecting biometric data as person-related data, it is necessary to constrain the possible consequences associated with its recording. As a result, it is desirable to avoid storage of the raw data, and to ensure compliance with the principle of data parsimony.

Storage of the data in a central register is currently precluded by statute for German citizens, although the establishment of central databases for aliens is not. Such centralised data storage would, however, involve problems in terms of data protection. This also applies to storage in decentralised registers. A question to be resolved is the relationship between AFIS (Automated Fingerprint Identification System) – which is also used to identify aliens – and the use of biometry in alien IDs.

There is need for political debate and action due to the fact that comprehensive implementation steps at all levels require planning and consideration of their implications at all levels, from issue through to control level. Further coordination processes at EU level and ultimately globally are required, if the goal is to achieve greater security without unreasonably impacting on global travel and data protection concerns. Another significant factor is likely to be the presence of German representatives on the committees of the International Civil Aviation Organisation and the EU, to provide their own input and defend national interests.

Consideration of the political, financial and organisational consequences of introducing and using biometric identification systems at all levels is still in its infancy. Comprehensive impact analyses would be appropriate here to provide guidance for political and data protection input for the developments currently in progress.

A comprehensive and complex project such as the biometric measurement of all German citizens and millions of aliens travelling to Europe or seeking asylum raises the question of acceptance. Considerations of technical practicability should accordingly be supplemented by the issue of societal acceptability. Numerous questions – for which there are so far few clear answers – would have to be addressed in a transparent public discourse. Greater clarity and a more nuanced approach are needed in particular for the question of what contributions which biometric documents can and should make to achieving which goals.

In the light of this discussion, consideration should further be given to the comparing the suitability of technical solutions and the justifiability of the different costs. A particularly important point here is to make clear that biometry can only make a limited contribution to improving security. Biometry is a technological approach for prevention and control, which means it is only one element (although an important one) in a broader strategy.

Public discussion is also needed in the conflict between security on the one hand and the goals of protecting privacy and limiting potential abuse on the other hand, which should also be reduced by technical and legal measures.

Finally, debate and decision should be expanded to include questions and objectives of innovation policy, working with developers and suppliers to formulate strategies aiming at the technological progression from the current document concept to a smartcard-based solution. For German companies, which are already well positioned in international competition, such a technically and societally innovative project opens up prospects of achieving competitive advantages with their own products and services.

A transparent public discourse could be a way of creating awareness of the importance of the dynamics of the societal and technological development involved in future intensive use of biometry.

The Office of Technology Assessment at the German Bundestag is an independent scientific institution created with the objective of advising the German Bundestag and its committees on matters relating to research and technology. Since 1990 TAB has been operated by the Institute for Technology Assessment and Systems Analysis (ITAS) of the Karlsruhe Institute for Technology (KIT), based on a contract with the German Bundestag

TAB

Office of Technology Assessment
at the German Bundestag

Büro für Technikfolgen-Abschätzung
beim Deutschen Bundestag
Neue Schönhauser Str. 10 · 10178 Berlin
Telefon: 0 30 / 28 49 10
Telefax: 0 30 / 28 49 11 19
e-mail: buero@tab.fzk.de
Internet: www.tab.fzk.de