This application track paper describes the key technology advances achieved through a component-based design process, meeting right on track all key requirements of management systems for biometric data, such as data protection acts, flexible user and device handling, installation, and operation functions, and grouping functionality for users and devices according to dedicated office environmental needs.
The key technology advances have been implemented in an application called BioLANCC. BioLANCC (Biometric Local Area Network Control Center) is a component based application and highly modular. Another key technology is the new Java-based biometric interface JBioDC, which will be discussed together with BioLANCC.
The use of biometric data to enable a personalized access control to resources, typically rooms, software packages, or systems, emerges due to a number of advantages. Those include a fine-grained tailored control, avoiding the problem of lost keys, or providing for customized access schedules for resources and persons.

Motivation

- Integrated access control for
  - buildings,
  - function rooms,
  - laboratories for personnel
- Traditionally use of hard keys

- Drawbacks of traditional approaches:
  - Large overhead:
    - Employee turnover
    - Loss of keys
    - Change of room access rights
Authentication may be performed by a number of different means. While knowledge and ownership describe the „traditional“ measures, the use of personal characteristics, typically termed biometric properties, becomes much more realistic in its broad and widespread use.

Technology has emerged, prices of biometric devices are decreasing, and the Internet as a means of world-wide communications across domains, serves as a transport medium of access control data and its supervision.
While multiple remote biometric devices are integrated across potentially arbitrary distances, BioLANCC is logically central management application. However, access to BioLANCC can be distributed, which allows remote administration. Existing applications for managing biometric data (VeriAdmin, FingerLAN) do only offer management for a particular manufacturer and cannot be combined with devices from different manufacture. Thus, integration is not possible with current biometric management application.

While local access control systems using biometrics are available today, e.g., in support of a single room access, mainly by applying finger print scanners, the interconnection of multiple of such local systems into a centralized management system has been developed partially in vendor-dependent systems. Thus, to cover a wide range of physical distances, e.g., for rooms scattered across a campus or many users located in different company offices around the world, and to cope with a large number of different biometric devices, such as finger print, iris, or face scanners, a new, flexible, and distributed approach became necessary.

Therefore, the communication based on Internet protocols serves as a bridge for the physical distance and a suitable as well as new control center manages the biometric data as well as user-specific and device-dependent management data.
The new management application development termed BioLANCC (Biometric Local Area Network Control Center) determines an important step beyond current management software packages for biometric devices, data, and users. This approach undertaken marks a revolution in biometric administration software due to a number of reasons.

Firstly, the TCP/IP-based networked collection and distribution of access control details of manifold biometric devices provides for a location-independent and device-unspecific integrative system. Multi-biometric support is enabled by BioLANCC through the integration of different biometric data into a single, per user-oriented and per device-driven management application.

Secondly, the use of object relational mapping libraries allow for a wide range of databases. In combination with the documented interfaces, external data sources from existing applications can be integrated.

### Overall BioLANCC Project Goals

- **Device-independent**
  - Integration of devices from different manufacturers
- **Support for many DBs**
  - Hibernate: Object/relational mapping
  - MySQL, PostgreSQL, Oracle, ...
- **Platform-independent**
  - Windows, Mac OS X, Linux, Solaris, ...
- **Open standards-based**
  - TCP/IP
  - Documented interfaces → Integration into existing applications
The remote scenario envisions a world-wide interconnection of access rules, associated to humans and users, where BioLANCC serves as the communication bus and exchange point for access control, supervising, and enrollment data.

The example presented shows three locations, which operate independently, and use a single BioLANCC system to maintain all personnel and visitor access data. The grouping concept of locations (biometric devices) and users is highly flexible for subgroups, overlaps, and monitoring groups.
Additionally, the BioLANCC control center has been designed as a fully platform-independent management application, running on operating systems such as Windows 2000/XP, Linux, various Unix, MacOS, Sun Solaris 10, and others. These possibilities have been achieved due to a standardized architecture using the Java platform, which is combined with a flexible and time-driven access rights and device management scheme for users and devices.

In support of the data storage for user and device data, BioLANCC integrates Hibernate and supports common SQL databases, e.g., MySQL, HypersonicSQL, Oracle, Microsoft SQL Server, DB2, Sybase, SAP DB, or PostgreSQL.

Various new biometric devices can be integrated via the open interface JBioDC (Java-based Biometric Device Connectivity).
BioLANCC uses the MVC pattern for the core components. The model is backed with the Java persistence framework using the Hibernate implementation. The view is split into a Java SE version and a Java EE version. The application server for the Java EE version is JBoss. BioLANCC uses many new features of Java 5 such as generics or annotations.

One key feature that makes BioLANCC flexible is the definition of interfaces to allow other applications to communicate. Report and user information can be stored / provided by any data source as long as it conforms to the interface defined in BioLANCC.

Scalability is an important requirement. As BioLANCC is logically centralized and the default setup does not consider scalability issues explicitly, the Java EE framework has been used to increase scalability by distributing components.
JBioDC stands for Java Biometric Device Connectivity and it is a high level API for communicating with biometric devices. In contrast to BioAPI and its wrapper JBioAPI which defines low and high level interfaces, JBioDC has a reduced set of interfaces. It is important to mention that JBioDC is not a standard, but future work focus on submitting JBioDC as a JSR.

JBioDC consists of 5 interfaces. The only mandatory is Connection due to the different nature of biometric devices. In contrast to SNMP which also defines a protocol, JBioDC only defines an interface.

One major problem is that no standardized biometric templates exist. Every vendor uses its own format and converting is often not possible. Therefore, the interface Template has only 2 mandatory fields: UserID and TemplateID and everything else is optional.
Finally, all events and actions performed at access control devices and within the management application are traced and tracked within BioLANCC to offer a powerful reporting and maintenance functionality. Besides a CSV-based export functionality a number of interfaces for a time management and reporting system have been integrated as well.
BioLANCC has been implemented with ease of use in mind. To achieve this goal, intensive usability tests have been conducted and the result has enhanced the appearance and the user experience.
In summary, the BioLANCC management application for biometric data provides the first world-wide platform-independent system in support of multiple biometric devices, flexible user and devices grouping, integration, and installation, and a TCP/IP-based network connectivity for resources across the world. BioLANCC is still under development, but it has already been deployed multiple times.

Conclusions

- Highly **flexible and distributed** biometric management system
  - First system world-wide **independent of devices** (JBioDC) and **OS** (Java)
  - Lower **costs instead** of physical key handling
  - No loss of **keys** and no sharing of personal resources

- **Target Markets**
  - **SMEs** (few devices, small number of resources/doors)
  - **Industry** (many devices, many locations world-wide)
Thank you for your attention!

Questions?

http://www.csg.uzh.ch/research/biolancc/