## D28 Biometric Devices and Software for Facial Comparison and Iris Matching: Use in Forensic Science?

*Zeno J. Geradts, PhD*, Arnout Ruifrok, PhD, and Rikkert Zoun, MS, Netherlands Forensic Institute, Laan van Ypenburg 6, Den Haag, SH 2497GB, Netherlands*

After attending this presentation, attendees will understand how the various aspects of biometric devices and the use of biometric software for face and iris comparison will impact casework.

This presentation will impact the forensic community and/or humanity by demonstrating the challenges in using these systems in investigations, and the information that can be extracted as evidence from digital traces in these systems.

The use of biometric properties in access control is growing. Nowadays these devices used for access to computers, sport clubs and of course the borders. The ICAO-standards for implementation in a biometric passport are an example of this. In these ICAO-standards, the specifications are given of the contactless chip and of the resolution of the images. As the storage in these chips is limited, the quality, due to the resolution and compression of facial images is not enough for a proper forensic face comparison.

Many implementations of biometric devices and software are available in commercial products, such as use of facial comparison, iris, finger prints, hand scanner, vein scanner etc.

With the use of biometric systems, the possibility to enter the biometric features in databases also exists. In this way, a person can be identified from the database. An overview will be given in this presentation of the biometric properties of such a system, such as false acceptance rate, false reject rate, failure to enroll rate.

For forensic science, it is important to know how the systems can be circumvented, since the digital traces from these devices might be used as evidence in court.

In theory, it would be easier to follow a person, and check if the person is actually there. However, a problem is that with the wide use of biometric systems, it becomes easier to spoof a fingerprint, or another biometric feature. Examples of spoofing biometrics are well known, and some of them can be easy.

For evaluation of biometric systems in forensic science, it might be useful to have databases of faces and irises, such as is also implemented in the widely used AFIS-systems. In Netherlands Forensic Institute laboratory, a widely used facial biometric system and an iris system were analyzed. The results of this research, with different properties of the systems, are presented.

Another field of research is the linkage of biometric properties. In practice, it appeared that on several commercial devices no encryption was used, which make it easier to sniff biometric properties such as fingerprints from the USB-connection.

To date, there have only been a few cases requiring analysis of biometric devices. One case was a PDA with fingerprint access control. To enter the system, a rubber stamp was manufactured from a slip of the suspect. It is expected that there will be more cases with biometric devices in the future. Current research focuses on the value of image databases for facial comparison.

**Biometric Devices, Iris Matching, Facial Comparison**

 ** Presenting Author*