Memo of Meeting

Date: August 7, 2002

Representing Daon, Co. of Dublin Ireland:

James Dunn, Senior Technical Sales Consultant
Martin Walsh, VP Regulatory Affairs

Representing FDA:

Charles A. Snipes, Compliance Officer, Center For Drug Evaluation and Research
Randall L. Woods, Compliance Officer, Center For Drug Evaluation and Research
George Smith, Jr., Compliance Officer, Center For Drug Evaluation and Research
Pat Beers Block, Consumer Safety Officer, Office of Science and Health Coordination, Office Of The Commissioner
Dennis M. Dignan, Consumer Safety Officer, Center For Food Safety & Applied Nutrition
Paul J. Motise, Consumer Safety Officer, Office of Regulatory Affairs

The meeting was held at the request of the Daon representatives, as a follow up the December 2001 meeting we held with them, to discuss their biometric electronic identity product in the context of 21 CFR Part 11. At the start of the meeting we explained that FDA does not formally review, approve or disapprove of products or services that enable people to comply with FDA regulations. We advised that the meeting would be an information exchange and that our comments should not be taken as formal FDA positions.

The Daon representatives explained that Daon continues to produces an electronic identity product designed with part 11 requirements in mind and initially focused on the pharmaceutical industry. The firm's system provides a biometric based front end to digital signatures and public key infrastructures (PKIs). Initially, the biometric trait will be fingerprints, with other traits to be folded into the product in the future.

During the meeting the Daon representatives explained how their system builds layers of electronic signature non-repudiation and how a single biometric based electronic signature can be used in a scalable computing environment to attain convenience of single sign-on. They explained how their offering can, in an identification management framework, be used to assign end users a set of role based privileges that establishments can centrally manage.

The Daon representatives emphasized the relative strength of binding an identity to a person that biometrics offers. They also explained that their system is designed to adjust to changes in biometric traits that occur over time. They explained how the biometric sensing device captures a number of physical attributes, making a falsified biometric trait more difficult to impersonate.

Regarding the relative security strength of their system, the Daon representatives explained that their product had attained level four (the most secure) of the Federal Information Processing Standard 140-2 (a U.S. cryptographic module standard).

During the meeting the Daon representatives reviewed the overall architecture of their system, the application interface and capacity for expansion.

The Daon representatives also briefly explained the results of a survey they sponsored to gauge the relative weaknesses of using identification codes in combination with passwords (without augmented biometrics). The survey was conducted by the Adelphi International Research Institute and involved interviews with some 30 clinical investigators and directors. According to the Daon representatives, the study showed password/id sharing, people signing for others under other people's id/passwords, and in general, a failure to take the resulting electronic signatures seriously.

The Daon representatives asked if FDA could formally recognize the relative superior security of biometrics. They commented that as long as FDA allowed for use of lower security electronic signatures in the form of id codes and passwords, potential customers saw no pressing incentive to adopt stronger methods.

We commented that part 11 implicitly recognizes the relative strengths of id codes used with passwords, digital signatures, and biometric based electronic signatures in terms of codified controls for each type of technology, but that by following proper controls required by the regulation, all the technologies carried equal legal weight. We explained why it would be inappropriate for FDA to effectively mandate use of one technology over another. We commented further that firms that are subject to part 11 may elect to adopt a variety of technologies they deem appropriate for their particular situations. We suggested that firms might adopt biometric systems when the advantages of doing so fit their own needs, and suggested that the case for adopting biometrics would have to be made by other parties – FDA would retain neutrality at this point.

The meeting lasted about two hours.

cc:
FDA Attendees
HFA-224
Part 11 Guidance Dockets

Doc ID DaonMemoOfMeeting080702.doc
P. Motise 08/15/02; rev 8/29/02