

The top example shows a pro-forma older style passport which of itself contains little reliability and could be readily forged. The lack of a photo and other coded data would not be considered adequate today.

The current passport is shown in the middle picture, containing the photograph of the holder and a machine readable zone which records the passport number along with some "biometric" and control information. (The term "biometrics" refers to data for an individual which is basic in nature, unchangeable, and not particularly sensitive. For example, one's name, picture, date of birth, and signature are all biometric information elements.)

In the lower picture is shown a passport ID page which contains a variety of options which may become the norm during the 90's. The technology to do this exists today. Special features include:

- o A digitized image first captured by the Passport from the picture submitted or from a video camera image capture. In any case, the image digitally imprinted on this page is the same that can be retrieved from central data files for renewals or inquiries.
- o A digitized signature block, machine generated after capture from the application form in a similar manner to the above. This signature could also be called up to screens as a result of renewals and inquiries.
- o An integrated read-only chip with special authentication features such as control counts and other self-checks. These features can be readily verified by appropriate readers, thereby directly increasing intrinsic passport security. The information on the chip can also be readily checked against central data bases for excellent extrinsic security protection as well. In this latter mode, note that no data on the passport holder need be released for authentication, only the control checks. Use of the chip, albeit expensive today, can render passports virtually non-counterfeitable with proper checking procedures.