Is the new e-passport safe?

Five reasons why the State Department and the Smart Card Alliance think so

1 MATCHED DISPLAY. Much of the information that appears on the printed section of the passport, including the bearer's photo, is stored on the chip and displayed on the screen reviewed by border officials. Border officials can check whether a traveler is trying to use someone else's e-passport chip information.

2 SIGNED AND SEALED. Passport agencies electronically sign the information on the chip and lock it to prevent tampering and to signal whether data has been modified.

3 READER CONTROLS. E-passport advocates note that the documents can only be read if they are handed over and opened. At that stage, a code embedded in the document's "machine readable zone" must be optically scanned before the e-passport chip communicates the data it contains. That process generates a one-time-use key that the system uses to encrypt the data transmission between the reader and the chip.

4 ANTI-TAMPER. The data in the chip is digitally signed by the passport issuing authority, according to Randy Vanderhoof, executive director of the Smart Card Alliance. That process "means that if the data is altered and rewritten back to any chip, then the electronic signature would not match the data that is associated with it. That would immediately flag that this is an altered passport," he said.

5 UNIQUE IDENTIFIER. The passport has been further secured by a modification to a standard ID feature that appears in all RFID units and smart cards. The feature consists of a unique identifier that the chip emits when queried by an appropriate reader. In normal RFID units and smart cards, this number stays the same and could be hacked by a sophisticated technician. In the U.S. passport's chip, the number changes each time it is read, foiling efforts to pinpoint U.S. citizens from a distance—in a crowd, for example.