CheapID

CheapID is a proposal to creating paper-based replaceable personal identity credentials.

The Technology
2D bar codes can store around 1Mb per letter sized sheet of paper.

Biometrics can supply a reasonable degree of uniqueness.

Public key cryptography can, correctly applied, supply both security and privacy.

The Synthesis
CheapID cards are cryptographically signed digital certifies printed on pieces of paper.

Because the cards are cheap and encrypted, they can be left behind to anchor contracts or authorize access.

Each card contains the identity information of the bearer encrypted with the public key of the applicable national court, plus a photo ID.

When the cards are presented, the signature on the ID checked, and the image presented, all without revealing an identity. A court order can be used to retrieve the identity escrowed on the card. This process can be done on a camera phone or a laptop.

Identity Services Architecture

To get these desirable properties in a way which could be deployed in chaotic environments means moving parts of the process to an international level.

Split Responsibility
National governments retain responsibility for identifying their citizens.

An international body takes responsibility for securely storing and searching biometric data for member countries.

National courts act as the interface to this database, limiting or preventing abuse.

Breakthrough Capabilities
By moving the heavy lifting of searching biometric databases to the international level, and offering it as a service, the Identity Services Architecture enables secure identity credentials to be issued nearly any circumstance.

By locking up identity information on cheap paper cards that are very difficult to forge or abuse for illicit identification, abuse of credentials can be limited.

By using paper IDs, laptops, cell phones and other commodity hardware, costs can be kept low, possibly far below $1 per issued identity.
Note that for issues of privacy and security, in the actual sequence diagram, much of the data is routed differently than it is on this diagram, although the start and end points are the same.
**Issuer Station**

Retains for each individual
Audit logs encrypted with the key of the National Court System.

No Access To
Any retained data.

**CheapID Card**

Retains for each individual
Court Key encrypted Certificate of Biometric Uniqueness.

Court Key encrypted Certificate of National Identity Number.

Unencrypted partial biometrics (usually just an image.)

Optional additional fields (certificates, possibly encrypted, for age or driving status.)

No Access To
Name. Other identifying strings.

**National Court System**

Retains for each individual
Depends on local administrative policies. In some states the court may retain a copy of each CheapID card it issues, including identifying biometrics. In others, the court may issue-and-delete retaining only audit logs, and rely on regenerating data if it is required (by, for example, resubmitting requests to the International Phenotype Database.)

The court is responsible for combining the various certificates generated by other levels of the architecture into a coherent whole in the form of the CheapID card. This does not mean it has to retain them, however.

No Access To
Government and Global Identity Database records except by due process.

**National Government**

Retains for each individual
Usual databases, including a National Identity Number or other identification string.

No Access To
Biometric data on individuals.

**International Phenotype Database**

Retains for each individual
Full set of biometrics.

Nationality.

Court Key encrypted Certificate of National Identity Number.

No Access To
Any data about the lives of the people in the database, including name.