Doing More with Less

A Strategy for Improving Trust in Identities in an Era of Tight Budgets
Governments leverage many forms of information...

Public Records

Other Government IDs

Commercial Information

Biometrics

...to establish one’s identity ‘footprint’
But each step of the identity process can be exploited...

- ‘Proofing’ documents can be fraudulent or fraudulently obtained
- Commercial ‘evidence’ of identity – utility bills, credit cards, bank statements – speak to ability to pay, not identity
- Biometrics don’t work for every person/application and some can be spoofed

- Knowledge-based authentication: possession of a key or correct information may be problematic
- ‘More secure’ identity documents may decrease vigilance and increase risk

... resulting in identities that cannot be trusted
A strategy for establishing greater trust in identities

- Start with solutions that consider the importance/value/risk of each identity and transaction
- Implement identity as a brokered service – tap into ID data where it resides rather than assembling a massive database of sensitive personal data
- Better use what already exists: clean up and leverage existing data
- Constantly monitor, assess and risk score the accuracy/integrity of data sources
- Conduct thorough and continuous vetting of every enrollee & user
- Obtain, manage and regularly update user consent
- Exceptions will occur! Solutions must handle them expeditiously to avoid security vulnerabilities
A Day in the Life of a **Trusted Identity User**

Sally is off to a business meeting with a client in another city.

Sally checks in at airport using her government ID.

Sally stops at an ATM to reload her bank card.

Sally leaves her house, locking up with a swipe of her finger.

Sally checks in at airport using her government ID.

Sally zips thru airport security via the fast-path lane.

Sally has lunch at a local deli, pays with her employee ID.

At destination Sally takes subway using her bank card.

Sally auto-registers in the client’s visitor system with her employee ID.

Sally stops by a local office after client meeting.

Sally uses her bank card to access her hotel room.

Sally buys from a vending machine with her employee ID.

Sally checks her eBay account using her mobile phone to pay via PayPal.

Sally checks into hotel using her bank card and government ID.

Sally checks in for her return flight using her government ID.

Sally stops by a local office after client meeting.

Sally authorizes stock sale with her mobile device.

After work Sally buys dinner with her bank card.

Sally unlocks and starts the car with her fingerprint key fob.

Sally checks into hotel using her bank card and government ID.

Sally stops by a local office after client meeting.

Sally checks into hotel using her bank card and government ID.

Sally accesses her corporate network using her employee ID.

Sally buys from a vending machine with her employee ID.
Questions/Comments?

Denny Carlton: Dennis.Carlton@us.ibm.com