Emergent Properties of User Managed Access to Personal Information

Kevin Cox
University of Canberra
ACT Australia
kevin.cox@edentiti.com

Abstract

This paper explores the outcomes from giving individuals control of and knowledge of their personal information held by others. The paper builds on the outcomes from the use of the idea to identify hundreds of thousands of individuals to meet Australian Anti-Money Laundering and Counter Terrorism Legislation. Specific outcomes are an increase in privacy, a reduction in costs, and an increase in functionality over traditional approaches to identification. The paper describes likely outcomes when the approach is used for other business tasks of proving the right to entitlements, of ensuring people comply with loan agreements and of providing health records of individuals for clinical treatment.

Introduction

User Managed Access (UMA) of data means that individuals manage the transfer of data about themselves when the data moves from one datastore to another. Typically the movement of personal data is through intermediaries such as banks (for financial data), recruiting firms (for credentials), taxation authorities (for payment of taxes), health professionals (for health information). UMA means removing control of the flow of data by these organisations and putting it in the hands of the individual (or user).

One way to implement UMA is to ensure that all transfer of data is via the user. This means if any personal information is to be transferred from organisation A, to organisation B, then the information must go via the user. This principle can be applied to any object. So if information about a company, a trust, horse, motor car, or a house is to be transferred it is transferred via the object.

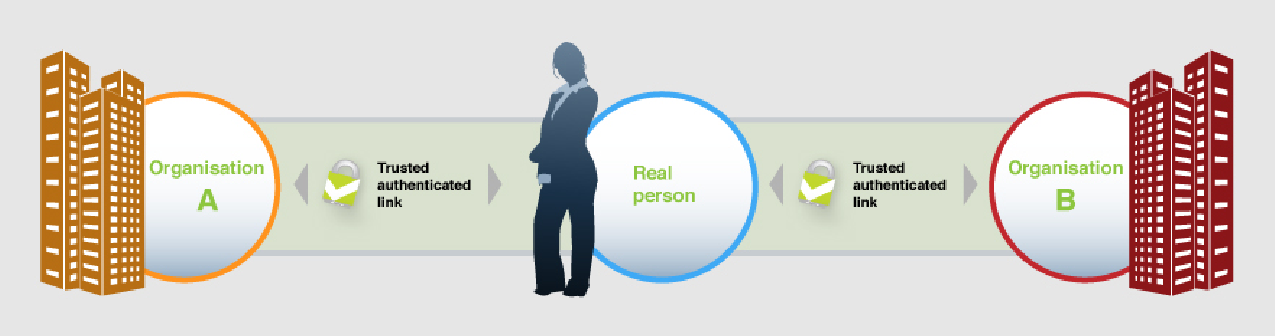


Figure 1: UMA access to personal data

The emergent properties of such an UMA implementation are:

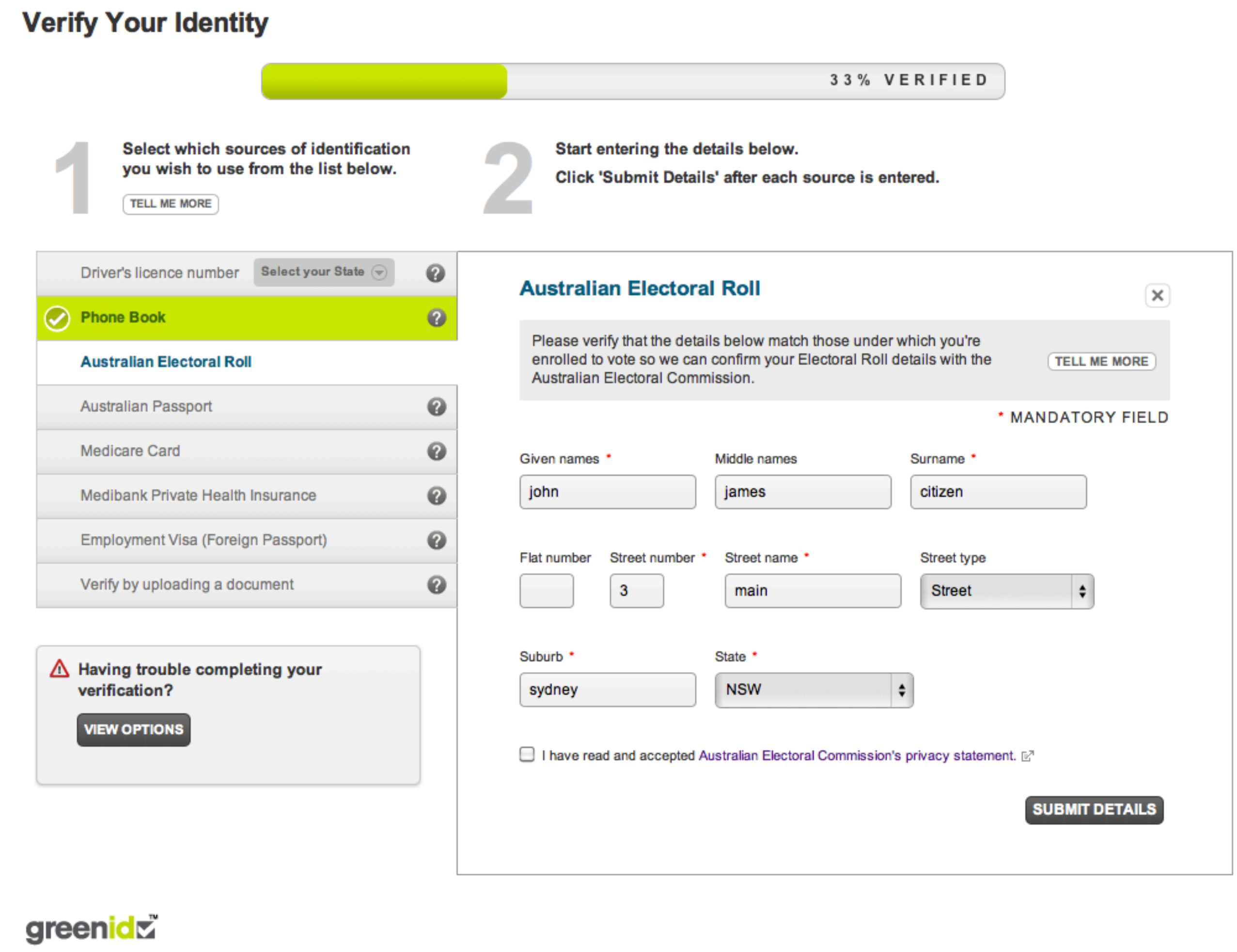
- Protection of Personal Privacy
- System complexity reduces from N squared to N
- The need for pre classification of data is removed
- Data stores can be logically integrated without any change to their internal structure or operation
- Transfers can take into account the transaction history of the individual or object
- The system evolves
- The legal structure supporting the system is built around two party agreements which can be covered by contract law.
- A reliable measure of Trust in Identification can be established. An Identity Trust Framework can be constructed around this measure.

Examples of these emergent properties are present in an operational system (greenID) to identify people for organisations who need to comply with Australian anti-money laundering and counter terrorism regulations. (see Chapter 4 of the Anti‑ Money Laundering and Counter‑ Terrorism Financing Rules Instrument 2007 (No. 1) AML/CTF).

An AML/CTF System for Electronic Verification of Personal Identity

This is a good piece of legislation in that it specifies the objectives of the legislation and leaves it to organisations to show how they comply with the legislation. To paraphrase the legislation it says that organisations must identify people commensurate with the risk of money laundering or financing terrorism. There are suggestions on how this might be done but the legislation is not meant to be prescriptive.

Figure 2 shows a screenshot of UMA based online verification system. To identify themselves the person chooses the data sources and continues to verify data sources until they satisfy the rules for identification as specified by an organisation.



Verify Your Identity

33% VERIFIED

1 Select which sources of identification you wish to use from the list below.

TELL ME MORE

2 Start entering the details below.
Click 'Submit Details' after each source is entered.

- Driver's licence number — Select your State
- ✓ Phone Book
- Australian Electoral Roll
- Australian Passport
- Medicare Card
- Medibank Private Health Insurance
- Employment Visa (Foreign Passport)
- Verify by uploading a document

Having trouble completing your verification?

VIEW OPTIONS

Australian Electoral Roll

Please verify that the details below match those under which you're enrolled to vote so we can confirm your Electoral Roll details with the Australian Electoral Commission. TELL ME MORE

* MANDATORY FIELD

Given names *: john
Middle names: james
Surname *: citizen

Flat number:
Street number *: 3
Street name *: main
Street type: Street

Suburb *: sydney
State *: NSW

□ I have read and accepted Australian Electoral Commission's privacy statement.

SUBMIT DETAILS

greenid™

Figure 2: Example screen from the greenID UMA based online ID verification system, where an individual is part-way through verifying their identity.

Once the person has verified their identity the fact that they have a verified identity is transferred to the requesting party. There is no need to transfer anything other than the unique identifier the requesting party has assigned to the individual and the fact of verification.

Protection of Personal Privacy

Any system that reveals private or personal information to another party, without their consent, automatically compromises privacy. The person with the private information has to promise not to share it and put in place systems to protect the private information. Protecting data is expensive.

With UMA systems personal data is only revealed if required. When UMA systems are widely used it is expected that less personal data will be kept in fewer places and some data, such as a verified biometrics, will only be kept on physical devices owned and controlled by the person.

In many transaction systems the only information that is needed by the requesting party is the verification status. It is expected that, as UMA becomes more widespread, systems will change so that personal data is only stored once in the originating system.

System Complexity

If personal data can be moved between organisations then the graph of interactions is complex as any organisation can interact with any other organisation.

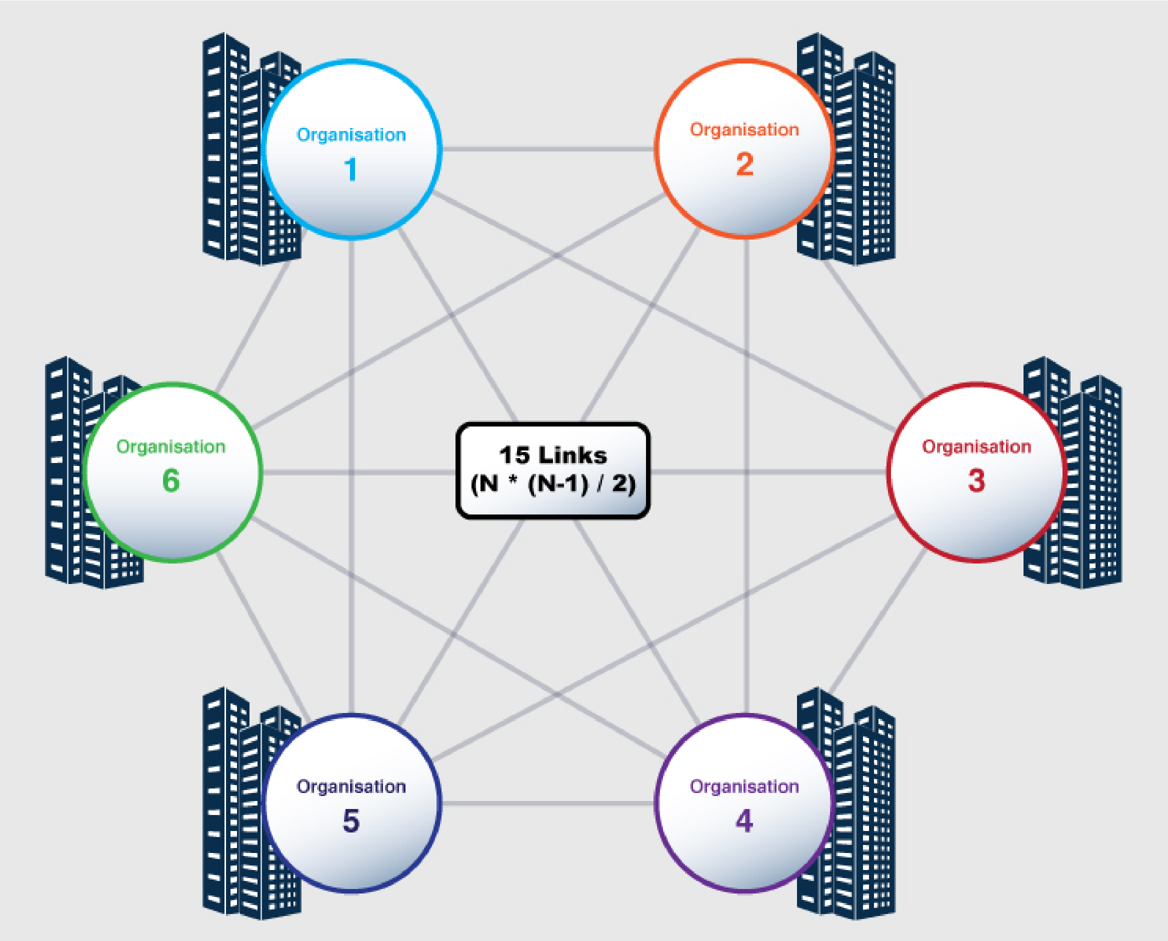


Figure 3: The complexity of a non-user-centric UMA system is demonstrated by the number of linkages required between each organisation

If all movement of personal data is through the individual, the complexity as measured by the number of pathways is significantly reduced

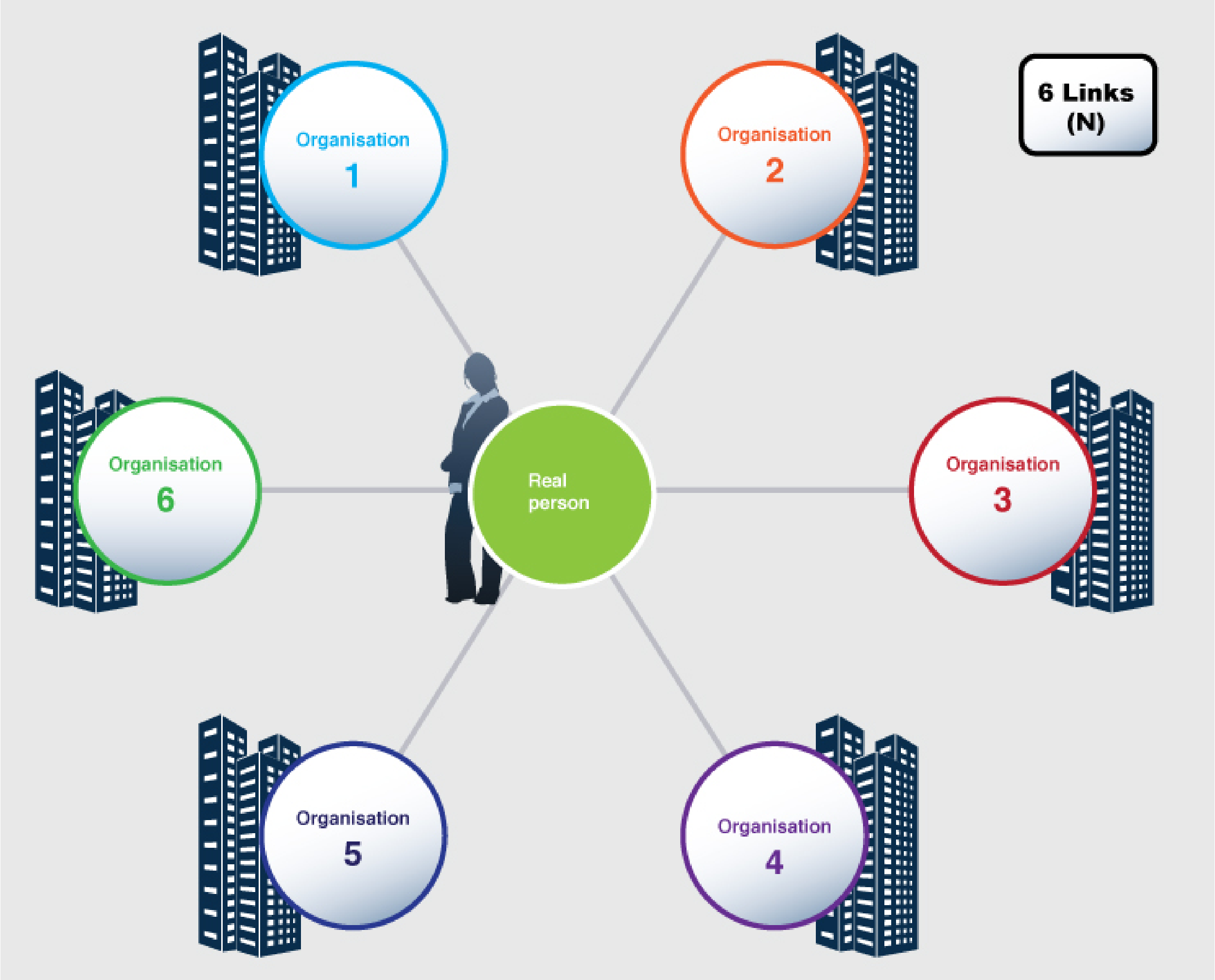


Figure 4: The simplicity of a user-centric UMA system is demonstrated by the reduced number of linkages required.

Once there are large numbers of organisations dealing with the same group of individuals the complexity of the organisation to organisation communication is of order N squared compared to the complexity N when personal information goes through the individual.

Classification of Data when Needed

When information is shared it is necessary for both sides to a transfer of information to agree on the meaning of information. This is typically achieved with a data classification system involving a thesaurus and each piece of information being defined and tagged with a classification. This approach to sharing of information is expensive and inaccurate.

If all transmitted personal information is passed via the individual concerned then the translation from one system to another can be performed at the time of transmission. If there is a common system used by all individuals then this automatically makes for a common translation mechanism. This is possible with today’s communications and computing power.

Data Systems integration without change

One of major barriers to implementation of sharing of data is the need for existing systems to change. For example, the introduction of a common id number for all health related matters is a significant barrier to deployment because existing systems have to be changed to incorporate another ID.

Using the approach of data always going via the individual means that existing systems do not have to change. They will need to be able to expose data and to consume data but internally the systems remain as they are. An example is when two organisations merge and there are efficiencies to be gained by getting a single view of a customer who has relationships with both organisations. With a UMA approach the existing systems can remain the same and integration can be built on top of these systems.

Transfers with Context

Transfer with context is the idea that, when information is transferred from one organisation to another via an individual, information from previous transactions (or context) can be used to assist in the translation of information. An example of the practical use is that if two transfers of information are initiated by an individual from physically separated locations, at about the same time, then one or other of the transactions may be bogus.

Change through Evolution not Revolution

If we have a system of always involving the individual in all transfers of information then it is possible for it to change in small steps or evolve. We can change the system individual by individual rather than requiring changes to occur for everyone at the same time. For example, if a government decided to change the tax laws they have to change the laws so that they apply throughout society even though the laws only applied to a particular group of individuals. Instead of global changes, the rules for particular individuals can be incorporated in the transfer rules person by person.

Legal Structures with Individual Contracts

The legal structure for transfers via individuals is established with agreements between a person and a single organisation or entity. There is no need to get agreement across multiple organisations before implementing a system. People and organisations can join one by one when convenient and each with different rules. This approach leads to a simplification of the legal framework because it is built on top of two party contracts.

Measuring Trust

Measuring trust can be achieved by measuring the number of times individual contracts are broken by either party and comparing it to the number of times trust is not broken. To achieve this, contracts need to have a notification process to an independent authority when the contract is breached.

When personal data is stored it must be given a unique identifier for each individual. With UMA identification can be achieved so that unique identifiers are only known to the individual and to the organisations using the identifier. If there is a breach of trust that required the knowledge of an identifier then one of the parties had to have compromised the identifier. Sometimes this can be determined by forensic examination sometimes not. If it can be determined then full responsibility for the breach of trust must be taken by the releasing party otherwise the responsibility for the breach is assigned to all parties who knew the identifier.

The fewer parties who know the identifier the easier it is to determine where the breach of trust occurred. The minimum number of parties is two. If every organisation that stored personal data used its own unique identifier for an individual then Trust in the system will increase and the Measure of Trust will reflect this increase.

A Community can increase Trust in Identity if many organisations use their own unique identifiers to store personal data and if they only allow access to that data through the individual concerned. When there are too many parties able to access personal data via the same personal identifier it becomes very difficult to make meaningful measures of breaches in Trust. With a UMA approach meaningful measures can be constructed that will reflect the perceived Trust in Identity systems.

Summary

This paper has described the emergent properties of the greenID verification of identity systems based around user managed access to personal data. To ensure the user has full control, the implementation requires all information about the individual to come to the individual before being passed by the individual to another organisation. The system displays the emergent properties of low complexity, just in time classification of information, evolution, simple legal framework, and no change to existing systems. Any system involving the transfer of data about any object or person can use the same approach.