

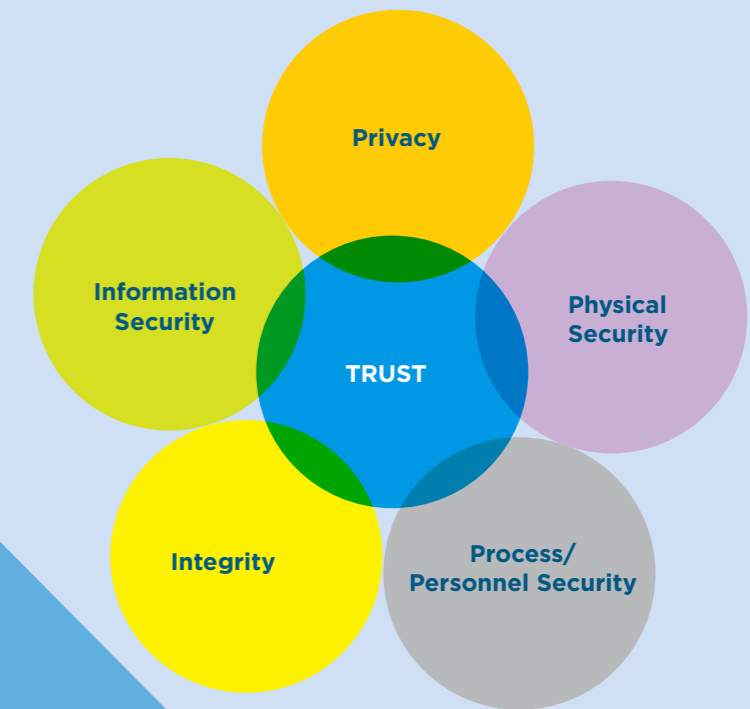
THE CHAIN OF TRUST:

MAKING SURE YOUR PERSONAL INFORMATION STAYS
YOUR PERSONAL INFORMATION

A CSC POINT OF VIEW



CSC



THE CHAIN OF TRUST: MAKING SURE YOUR PERSONAL INFORMATION STAYS YOUR PERSONAL INFORMATION

DEGREES OF TRUST

Working with many clients over the years, I was once issued a security pass with my details on it, but with somebody else's photograph. Having noticed the problem quite quickly, you might find it surprising that I then had a hard time convincing the issuing officer that the photo was not me, and that I needed a new card!

Now think back for a while: have you ever played that parlour game, the whispering one, where all the players line up side by side? At one end, somebody whispers into the ear of the person next to them "I'd like a cup of coffee and a cake", who then whispers it to everybody else in the line, until, at the other end it has morphed into something like "the stake was on a high fence"?

Imagine now the number of staff and computer systems that handle your personal information as you transact with different government bodies -

Federal, State or Local, Australia or worldwide. What do you expect of them? Presumably that you details are recorded carefully, shared only when necessary and, when you check them, you find they are always the same, and always what you told them.

You certainly don't want the government equivalent to the whispering game.

CHAIN OF TRUST

Making sure that your personal information is captured correctly, including that you are who you say you are, that it is stored and transmitted securely, that it does not get mistakenly altered, that it looks the same when recorded in different places, are all part of a concept that is called the "Chain of trust". The "Chain of trust" means that you can trust that the integrity of information is preserved as it is handed down the chain of people and organisations which need to use it. This may be to pay you a benefit, collect your tax or assist your business.

We normally have high expectations of the "chain of trust" in our dealings with government. Court cases have been seen to collapse if evidence has not been handled and reproduced in court carefully and without tampering. Imagine how our faith in government would collapse if we were presented with the wrong information "on file". Remember back to my ID badge with the wrong photo?

AT RISK

It is not sufficient to think only about "me" and "you" in any business relationship. In your dealings with government, there is always a risk that there are some unwanted "others". The "others" are the instigators of Identity Theft, Hacking, Phishing, Social Engineering, Cyber-Terrorism, and other malicious threats that can steal and misuse your information. And you might not know this has affected you until a long time afterwards.

Just as our day-to-day lives have been transformed through technology, the business of crime has also undergone a transformation by that same technology. Our information is managed in computer systems, and these need safeguarding so that they are no longer vulnerable to these kind of attacks, and remain secure as the threats and countermeasures change over time.

REINFORCING THE CHAIN

Learning from my own personal experience that I described earlier, the integrity of the "chain of trust" does not happen by accident, and is, unfortunately, not always an unbreakable set of bonds from one end of the chain to the other. A weak chain of trust, as we have seen, can result in more than just my own personal inconvenience. Multiply that by a population of 21 million people in Australia, and you have a significant challenge on your hands. Creating that unbreakable chain takes a lot of care and a lot of experience. And it takes vision.

VISION INTO ACTION

A strong chain means strong at the beginning, strong in the middle and strong at the end.

At the very beginning, one needs a strong idea of the whole system: a strong architecture or blueprint for the citizen-government transaction. This includes things like:

- The policy we wish to follow
- The legislation being enacted
- The business process we wish to execute
- How it affects customers, staff and other stakeholder groups
- The environmental threats and vulnerabilities we are subject to

WHAT CAN GO WRONG

A strong chain of trust from the beginning means personal and private information must be collected carefully and efficiently. The collection process must be performed securely, with respect for the rights of the individual, and, more and more, subject to informed consent.

This means that I'm willingly giving you this information because I know what you are going to do with it, and I trust you will look after it. What makes this happen?

- **Privacy** when gathering information, so that it cannot be overheard by potential identity thieves, and with respect for the often divergent privacy preferences of boomers, gen X, gen Y and so on
- **Integrity**, which means that information collected itself can be trusted, and amounts to sufficient proof of identity. This is the origin of the 100-point check, and significant automated mechanisms to check the veracity of documents, biometric matching against existing enrollees, and cleansing of old duplicate records
- **Information security**, so that the data is encrypted so nobody can read it, digitally signed so nobody can tamper with it or misrepresent it



CSC'S PROPOSITION

When it comes to deploying a secure chain of trust, CSC is the preferred partner for Federal, State and Local governments around the world.

We have experts and business solutions in areas such as the deployment of large government business transformation programs, security architecture and technology leadership. Working with CSC means that the chain of

trust is reinforced and extended beyond the boundaries of your own organisation, not only to CSC, but to other government agencies, non-governmental organisations and the public at large.

To learn how to turn your vision into action, talk to our experts at CSC or visit www.csc.com.au

- **Physical security**, so that equipment, and information is physically locked away so nobody can take it to their own basement labs for reprogramming, or unscrambling at their leisure
- **Process and personnel security**, so that separate staff members get involved to avoid collusion, and so that any computer security is not undermined by weak operational process or policy that was overlooked when the deadline loomed, and which is often the "weak link in the chain".

In the middle of the chain of trust, our customers expect that their personal information stays personal. In Federal government this means that it is only used for the purposes for which it was intended.

That my neighbour cannot look up my information without good reason, and that agencies can only share my information when they have been explicitly given legislative permission to do so. This means that at each government touch point that you or I go to, my information is complete and correct. And when it changes it is easy

for it to be updated everywhere that it is stored (and in the future, this may eventually be stored in a single place.) This can be achieved by means of:

- **Issuance of a strong token.** Be this token a long and complex reference number, a plastic card, a passport, a licence, a digital counter or anything else which can uniquely identify me, and which can save time at the shopfront, but which at the same time is difficult to copy
- **Comprehensive monitoring and audit** to record who does what, when, and to immediately detect disallowed or fraudulent patterns of behaviour

Issuance of a strong token can be costly, and provokes valid privacy concerns that need to be addressed to ensure citizens opt-in. But an alternative would be the equivalent of the enrolment process - name, address, 100-point documents, and biometric integrity checks and so on every time you presented yourself to a counter. With the busy lives people lead, and the general desire to save time, it is easy to see why a token, or biometrics, are usually considered necessary, albeit with privacy safeguards.

At the end of the chain of trust, our personal information needs to be handled with care, so that it is preserved in line with the necessary record keeping requirements and policy. And I want to be sure that my data is finally destroyed when no longer needed. Indeed by this time, the information will have been subject to numerous rules and regulations, all of which can normally be automated and easily audited with the right know-how. Examples might include:

- The Archives Act
- The Privacy Act
- The Attorney General's Protective Security Manual (PSM)
- The DSD issued Information Security Manual (ISM), designated ACSI-33
- AGIMO issued standards for e-Government, including the National e-Authentication framework and the Australian Government Architecture
- Industry standards for technology security, information interchange, secure tokens and biometric capture

All in all, preserving the chain of trust takes a well thought through architecture, and the governance model to enforce this over the long term.

Worldwide CSC Headquarters

Australia
26 Talavera Road
Macquarie Park, NSW 2113
Australia
+61 (02) 9034 3000

The Americas
3170 Fairview Park Drive
Falls Church, Virginia 22042
United States
+0 703 876 1000

Asia
139 Cecil Street
#06-00 Cecil House
Singapore 069539
Republic of Singapore
+65 6221 9095

Europe, Middle East, Africa
Royal Pavilion
Wellesley Road
Aldershot, Hampshire GU11 1PZ
United Kingdom
+44 (0) 1252 534000