



Early thinking: Operational governance for trans-Tasman e-Invoicing

Submission by Simon Foster, CEO on behalf of Squirrel Street

Background

Squirrel Street is a provider of online receipt and invoice management via the use of proprietary scanning, OCR and machine learning technology, servicing customers in Australia and NZ. Our customer base is primarily micro-businesses and we receive documents via post, email, mobile app, web upload and cloud storage integrations. We have almost 80,000 customers on a combination of free and paid subscriptions and integrate with the major SME cloud accounting platforms.

The e-Invoice Framework offers a far more cost effective and accurate method of receiving Tax Invoices on behalf of our clients, and we expect that e-Invoice adoption will allow us to grow our micro-business customer base, as well as provide them the ability to automate the delivery of invoices to their customers.

Squirrel Street CEO, Simon Foster, has been a participant in various Digital Business Council Working Groups since their inception in January 2016, a Board Member of ABSIA since April 2016, is currently Treasurer of ABSIA and Vice-President-elect for 2019 and ABSIA's representative on the Digital Business Council. Simon is also on the Board of the Pearcey Foundation, and has previously held board positions with the Australian Computer Society and Service-Manager's Asia-Pacific. Simon holds a BSc (Comp Sci) from UNSW, and has held senior management positions in Europe and Asia Pacific at software vendors including DoubleClick, Mercury Interactive, Lycos Europe, Schneider Electric and BlueFreeway.

QUESTION 1 – What do you consider to be significant policy or legal barriers to the implementation of e-Invoicing in Australia and/or New Zealand?

e-Invoicing is most likely to be successful with a large and diverse ecosystem of software vendors participating in various parts of the network – be that as a Digital Capability Publisher, Access Point or Business Management System and various API partners to accounting software. It is critical that the policy direction encourages participants of all scale, and that a balance is achieved between access to the network and information and business security requirements. The variety of offerings in the ecosystems of SME cloud accounting vendors has been a significant driver of their growth and consequently SME productivity in Australia and New Zealand. Given the focus on value for SMEs provided by e-Invoicing, a similar approach is required.

QUESTION 2 – What do you think would be the best legal structure for the operational governance body?

In our view it is essential that the operational governance body be an Incorporated Entity for the reasons already outlined in the consultation document. Of the various incorporated entity types across Australia and New Zealand, our preference would be for a New Zealand Limited Company. The reason for this is that NZ Companies House provides free and transparent access to information about companies in contrast to Australian equivalent organisations at both State and Federal level.

QUESTION 3 a) – Beyond the initial establishment phase, who do you think should lead the operational governance of trans-Tasman e-Invoicing; and what functions and roles should the operational governance arrangement include?

Our view is that a broad cross section of the consumers, developers and regulators of the eInvoicing Network should be involved. That would include business (suppliers and customers, both large and small), intermediaries (accountants & bookkeepers), business software developers and operators of e-Invoice access points, government agencies and relevant industry associations. Noting that government agencies are relevant as regulators in addition to their role as significant users of the eInvoice Network.

Functions of the operational governance body should include:

- Maintenance of the e-Invoicing Framework, itself.
 - o The Digital Business Council working groups provide a good structure for this work and their terms of reference already define well the detailed tasks required.
- Accreditation of DCPs and APs in the eInvoice Network
 - o Accreditation of DCPs and APs should be both technical (conformance to the framework) and operational (eg implementation of appropriate information security controls, business viability and probity of directors/owners)
- Ensuring the trust, security and reliability of the e-Invoicing network
- Adoption of the e-Invoicing Network
- Dispute resolution between participants in the e-Invoicing Network
- Expansion of the e-Invoicing Framework into other business digitalisation arenas. The Procure-to-pay process and its partner order-to-cash are the obvious next steps.

Operational governance will likely need multiple sub-committees to make recommendations to a Board, plus a staff capable of performing secretariat functions, research on standards and oversight of accreditation.

While operational governance models exist in other jurisdictions, notably PEPPOL in Europe, the focus for e-Invoicing in Australia & New Zealand is substantively different. We commend the Australian and New Zealand governments for giving attention to B2B relationships, and particularly SMEs. This can take advantage of the significant penetration of cloud accounting in SMEs across Australia and New Zealand, and the ease of access that the related ecosystems provide. This should allow local software vendors prove their offerings in the trans-Tasman market and build export opportunities as the rest of the world catches up.

QUESTION 3 b) – Do you see sufficient incentive in our proposal for you to consider participating in the operational governance body?

There is no particular incentive in the proposal that specifically attracts us to participation. However, the fact that participation means influence over and awareness of the direction of e-Invoicing is attractive both from an altruistic and commercial perspective.

QUESTION 4 – How do you think the long-term sustainability of the operational governance of the trans-Tasmania e-Invoicing, with appropriate cost allocations, can best be assured; and what funding models do you suggest?

The particular focus on SMEs presents a challenge. It is expensive to market to and acquire SME customers. Our existing offering to SMEs which involves physical scanning, OCR & human verification retails at under 40c per transaction. To drive e-Invoice adoption the cost to SMEs will need to be orders of magnitude less than this and trending to zero.

In contrast, the current cost per transaction for Enterprise and Government (as a processor of invoices rather than a regulator) is stated by research conducted by the DBC as being in excess of \$40. Anecdotal evidence from our conversations with large companies is that the cost is often substantially higher than this.

As the largest savings will be made by enterprise and government, the cost of both implementation and operational governance should be borne there. Models exist in other jurisdictions of levying fees to access points and other network participants to cover ongoing governance costs. There are also examples in other areas that are superficially similar – eg domain name registration – where relatively low-cost levies upon each business using the network (ie sending an e-Invoice) may generate enough income to sustain governance.

However, we believe this is a consideration for the future once e-Invoicing has achieved ubiquity. Current customer acquisition models rely on entirely free offerings, or 30-day trials. The introduction of a fee at this early stage of market development may stifle it before it has begun.

QUESTION 5 – Do you have any additional comments or information to assist with reviewing and further developing our early thinking and conclusions about a preferred option for operational governance of trans-Tasman e-Invoicing?

We have heard particular concerns expressed about an increased likelihood of false invoices being transported by the e-Invoice Framework. We believe that remedying a missing component of the e-Invoice Framework will result in the reverse being true – that false invoices will have a significantly smaller likelihood of existing on the e-Invoice Framework. This technology is secure signing of messages allowing for a confident, validated and non-repudiable identification of the originator of an e-Invoice, and verification that the content of the message has not been tampered with.

The inability to reliably identify the originator of an email is a significant cause of the continued prevalence of phishing and other cyber-attacks and has been for a long time. This article is almost 10 years old, but the description of the problem, and why the technology to solve it has not been implemented, has not changed much in the interim -

<https://www.theguardian.com/technology/2009/jan/08/phishing-email-security-settings-digital-signatures>.

What has changed in the last decade is that the technology to sign and encrypt messages has become cheap (often free) and easy to implement. Projects such as Lets Encrypt from the Internet Security Research Group (<https://www.abetterinternet.org/about/>) which sought to make secure websites pervasive by automation and free certificates has been very successful with 76.5% of websites globally now using secure technology, compared with 50% only 2 years ago (<https://letsencrypt.org/stats/#growth>)

The risk of leaving this implementation to later is that some players may consider it too hard to retrofit. More-over, including signing of messages from the beginning can reduce some of the governance requirements, as the ability to tamper with messages in transit, impersonate another party or generate fake invoices will be substantially reduced.