e-Invoicing Governance Feedback

Response to Treasury Discussion Paper

November 2018

Preface

This submission is in response to the Treasury's Consultation discussion paper on e-Invoicing. It contains both higher level comments and answers to the specific questions.

This paper is accompanied by a technical paper which was submitted two weeks ago in response to the ATO's e-Invoicing request for feedback covering overall technical deficiencies in the DBC standards.

Table of Contents

1 Background

Layer Security submits this feedback with significant interest and expertise in security and privacy and significant experience in e-Invoicing and the underlying ebMS3/AS4 technology.

At the technology level, Layer Security is a major supplier of SBR2 and e-Invoicing messaging components to software suppliers and service providers. This technology underpins major services and systems such as:

- Cloud providers e.g. Xero (SBR2 services for tax and STP)
- Gateways e.g. Ozedi (e-Invoicing, SBR2 services for superannuation and STP)
- Financial systems e.g. MicroTax, Astute Payroll, DataComm etc.

At the advisory level, Layer Security has been involved in:

- DCL pilot (2018)
- E-Invoicing pilots (2018)
- ATO Digital ID Working Group (2018)
- ATO DARG – DSP Architecture Reference Group (2018)
- ATO Operational Framework Working Groups (encryption, authentication, 2017)
- DBC Standards input (2016)

At the expertise level, Layer Security staff have significant career experience (30 years) in the development of large-scale distributed security and communications products (for global banks, carriers, governments, corporates). Staff have also been involved in many international standards groups.

As Layer Security works with a broad range of DSPs (Digital Service Providers), it has wide and important experience in standards and governance. As such, it can represent much of the market, particularly the smaller players that don't get a voice, and to highlight necessary security and privacy requirements that is often played down by bigger (vested) players.

Note that Layer Security was the first vendor to publicly demonstrate DBC messaging, complete with end-to-end security, at the ABSIA 2016 conference.

2 General Comments

The world has moved on since 2016 when the DBC Framework was first formulated. Back then, security, privacy and end-to-end messaging were seen (by the DBC standards setting committees) as impediments, so these got minimised or made out-of-scope. The nett result is a minimalist set of standards, deficient in security and privacy safeguards (which any expert review would also conclude).

In terms of governance, the removal of security and privacy features in order to make it simpler to participate will lead to the *opposite* outcome. The DBC standards are arguably so insecure that all kinds of complex legal governance may be needed to compensate (e.g. levels of accreditation) - and this presents a higher barrier to entry than a system that was designed to be secure in the first place!

In terms of safety, the lack of security and privacy features opens up the DBC system to various type of fraud and abuse.

- The lack of *message signatures* (the DBC made it optional) is in violation of the international ebMS3/AS4 standard. This poor decision opens up the risk of (undetectable) message tampering.
- The lack of *end-to-end payload signatures* (CMS) associated with strong credentials means that received invoices cannot be verified against the claimed seller identity. This opens up the risk of impersonation fraud.
- The lack of *end-to-end encryption* means that Access Points are privy to every business transaction. This can be exploited by service providers who can sell business intelligence about any business to competitors or to the multi-billion-dollar (largely invisible) “big data” data-broking industry. Note that privacy controls may not be enough here, because they would only cover specific details, not aggregation and insights. (Knowing the invoice details of a business can reveal a lot of sensitive information about that business.)
- The lack of *end-to-end encryption* means provides Access Points become a honey pot for attackers who would target the very commercially sensitive information visible to intermediate Access Points. (The DBC Framework sends all invoices in the “clear”).

In terms of openness, the lack of end-to-end messaging means that the endpoints (Corners 1 and 4) are locked into their providers (Corners 2 and 3 respectively). This restriction limits the DBC network to just the big players. AS4 should be explicitly allowed by C1 and C4.

In terms of trust and confidence, if security and privacy features were mandated, then this would encourage participation because the network would be seen as much safer. This would also put Australia at the forefront of global initiatives to build large-scale, secure and private digital business networks.

Please see the accompanying document (LS-DBC-review-Oct2018.docx) for technical details.

3 Specific Comments

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 (including NIL confirmation)?

The main challenges are security, privacy, identity and openness.

Security means *mandating* minimum levels of security. It must be mandated as security can't be voluntary (à la seat belts were never worn until they were made mandatory). The minimum level needs to ensure safety of the entire system (à la a "roadworthy" is a condition of driving on the roads). For example, the ebMS3/AS4 standard mandates message signing (to safeguard the authenticity and integrity of messages) but the DBC has (wrongly) made this optional.

Privacy means end-to-end encryption (E2EE). E2EE is a proven way of safeguarding data as it travels across a network. It adds an extra layer of strong security and privacy, as E2EE effectively locks data up in a tamperproof package keeping it protected and hidden from all intermediate parties. But, the DBC standards do not contemplate this. Instead, the DBC standards define data (invoices) to be sent in the "clear" allowing any intermediate parties to be privy to every transaction of every business message being sent. This opens an attractive avenue for message provider exploitation – getting intelligence about business data which could get (silently) sold to competitors or to the multi-billion-dollar (largely invisible) "big data" data-broking industry. The DBC Standards need to add this as an option, as many potential e-Invoicing participants are refusing to become involved unless E2EE is available.

Identity means having a trusted credential in order to ensure authenticity of messages. The DBC framework does not contemplate this. The TDIF is addressing this including how to recognise both government-issued and commercially-issued credentials. The DBC Framework needs to address this to prevent fraudulent messages.

Openness means end-to-end messaging. The DBC standards only contemplate corner 2 (C2) to corner 3 (C3). This locks in C1 to their provider (C2) and C4 to their provider (C3). In a real messaging system (as ebMS3/AS4 was designed) messages can travel end-to-end (C1 and/or C4 are AS4 clients). The DBC Framework needs to explicitly allow for end-to-end messaging to open it up to the smaller players.

Question 2. The best legal structure for the operational governance body?

The governance body needs to be independent, have clout and be properly funded.

The first option is government. The ATO has clout and hence can enforce proper governance around SBR2. However, it appears that the government has little interest in overseeing B2B, even though government is a huge buyer in this market and hence has a huge vested interest in proper security, privacy and governance of the DBC network.

The second option is a not-for-profit unlisted public company limited by guarantee (like GNGB) along with appropriate laws to compel compliance.

It is noted that the current DBC has no mandate, no legal structure and no funding, so this is the worst possible situation.

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?

Since the governance body must represent the entire industry, it must have representation from the wide spectrum of players in e-Invoicing including suppliers/buyers, software/services, government, financial industry, small players etc. These representatives must, in turn, cover the full range of expertise in legal, commercial and technical realms.

If the legal structure is government, then it should follow the example of the ATO who has good established processes for industry consultation and accreditation. Though there are problems here with true representation across the industry (as SBR2 clearly has the ATO's interest first and foremost).

If the legal structure is an independent incorporated organisation, then it needs to follow the example of the GNGB who has good established processes for industry consultation and accreditation. Though there are problems here with vested interests.

Note that a hybrid model may be required – as standards setting, accreditation and governance are three separate regimes with conflicting priorities and independence.

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

Yes, for technical standards setting – because this area is excruciatingly deficient in many areas relating to security and privacy. In part because of the lack of expertise and experience with the group that originally set the DBC standards.

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

If the legal structure is government, then it needs to have guaranteed allocations.

If the legal structure is an independent incorporated organisation, then funding could be via government grant, and/or a levy on accredited providers.

Question 5. Do you have any additional comments or information to assist us with reviewing and further developing our early thinking and conclusions about a preferred option for operational governance of trans-Tasman e-Invoicing? If so, please provide your comments here and/or direct us to the additional information you would like us to consider.

See Section 2 "General Comments".

About Layer Security

Layer Security develops security and privacy software modules that are easily embeddable into business-to-government (B2G) and business-to-business (B2B) applications.

The software suite includes a multi-functional server (LS-Server), embeddable clients (LS-ATO, LS-B2B) and supporting tools (LS-KeyTool, LS-CmsTool). Each is renowned for being powerful, yet small, fast and efficient, as well as being easy to install, configure, manage, and integrate. They have been widely embedded into third-party software products and cloud services including payroll, accounting, superannuation and e-invoicing applications.

Layer Security staff have extensive experience and expertise in security, privacy, networking, protocols, cryptography, encryption, certificates and key management. They have also contributed to many international standards committees and Australian Government advisory panels.

All technology developed is modular (small, standalone), portable (Windows, Linux) and compliant to a wide range of international standards (ISO, IETF, OASIS) and Australian standards (SBR, DBC). The technology is available via distributors.

Layer Security Pty Ltd
ACN 602 982 892

https://layersecurity.com

Disclaimer

Whilst every reasonable effort has been made to ensure that the material contained in this document is correct at the time of first publication, the information in this document is provided without warranty, either express or implied, of accuracy or fitness for purpose. You hereby release Layer Security Pty Ltd its officers, employees, agents and contractors from all claims, liability, damages and costs howsoever described arising out of or in connection with your use of this document.

This document may be updated without notice. By retaining and using this document, you accept the above conditions.