

# THE POST OFFICE IN THE DIGITAL TRUST FRAMEWORK

BY

TIMOTHY GRAYSON

Let's accept the notion that "[Identity is Center](#)," suggesting that information technology and networked computing is path-bound to resolve the evermore obvious identity obstacle. By implication there is an absence of trust impeding further commercial growth or evolution of the Internet; were it not so, present challenges would be moot and an online honour system would prevail. If true then the prevailing trust framework is inadequate and the digital world requires a new structure around which to form a commercial identity solution. This paper expands on the notion of a digital trust framework explored in an essay entitled, [Toward a Digital Trust Framework](#).

Trust is a social virtue which is essential to efficient commercial activity because it reduces transaction costs. It has that effect because, as Fukuyama notes: ". . . people who do not trust one another will end up cooperating only under a system of formal rules and regulations, which have to be negotiated, agreed to, litigated, and enforced, sometimes by coercive means. This legal apparatus, serving as a substitute for trust, entails what economists call 'transaction costs.'<sup>1</sup> But direct trust is not always achievable in practice anyway – particularly online where people are distant and detached in the extreme. To reduce transaction cost by effect of trust then, some structure for engaging "derived trust" projected by a trusted third party (TTP) needs to be implemented.

---

<sup>1</sup> Francis Fukuyama, *Trust: The Social Virtues & the Creation of Prosperity*. The Free Press, 1995. p. 27.

## A Digital Trust Framework

A digital trust framework has several essential aspects as depicted below. The foundation of *Beliefs* and *Values* is core to who we are and how we think: socially, commercially, etc. There is a primary superstructure on this foundation that includes *Security* and *Privacy*, which together create *Credibility* and support commercial success.

While sufficient in most physical-world instances, this framework is wholly inadequate in the digital world because of the many special characteristics and peculiarities of the online environment.

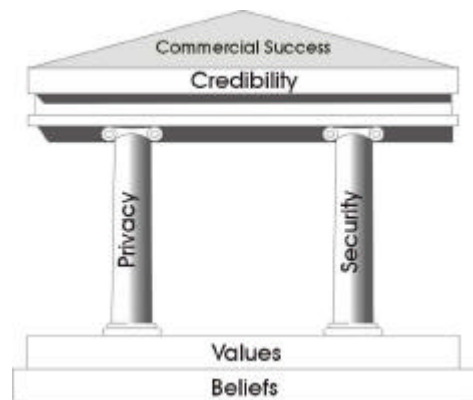


Figure A

Inclusion of several other functions would resolve the inadequacy and support a *digital* trust framework. These are: *Authentication*, *Attestation*, *Mediation*, and *Responsibility*. *Authentication* is the role of digital identity writ large in the broad world beyond the enterprise, including initial authentication and subsequent authorization of credentials. *Attestation* is the act of witnessing and attesting to the veracity of the

identity(ies) and the transaction(s). *Mediation* is the orchestration and chronicling of indisputable multi-party, multi-iterative electronic transactions. *Responsibility* encompasses the broadest notions of liability acceptance for digital transactions. All of these functions are best served by an independent TTP.<sup>2</sup>

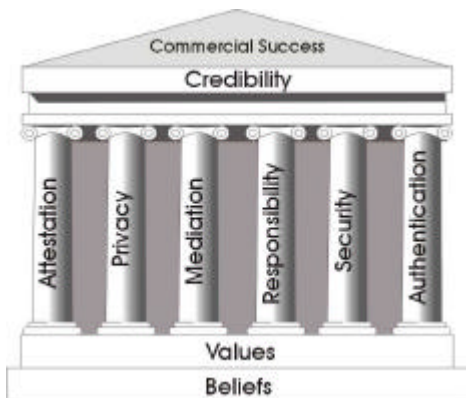


Figure B

This framework, or some equally robust set of functions encompassing not merely technology but also business process and (digital) social intercourse, will take shape no doubt. Our concerns about how that happens are at least two-fold. First, a framework evolving haphazardly will go through a series of misguided adventures pressed on by various powerful interests. It is also likely that the technology-centric debates about scalability, federation, standards, enterprise v. public identity solutions, etc. (all good in their own right) will hijack the broader discussion of a social trust framework. And, this digital trust framework notion has greater social and commercial breadth and import than “trusted computing” and so forth. Second, the issue here is the *absence* of trust, which we seek to mitigate with an institutional or structural substitute. But neither technology nor process nor standards nor policy is individually – or are they collectively – sufficient to achieve the *effect* of trust. The solution *needs* the third parties that can project their own existing trust onto the various structures, processes, and systems universally to engender the derived trust required to

claw back transaction cost increases that have resulted from the absence of social trust in the online world.

### Enter the Post Office

The venerable post office: a national institution that is so well trusted it’s the *sine qua non* of physical communication. Post offices range from government agency ([USPS](#)) through to private enterprise ([Deutsche Post](#)) and variations in between (e.g., Crown Corporation in [Canada](#) and the [UK](#)).<sup>3</sup> In all cases, the post office is a disinterested transporter of private information. It does not open the mail – legally it must protect that matter in its possession, and its structure for universal delivery is the result of hundreds of years of development.

The world’s post offices share other assets beyond this “trust” goodwill that are ready to be exploited in the service of a digital trust framework. Consider:

- Physical and electronic infrastructures that are secure and designed to protect information.
- Legal right and obligation to enforce and maintain high standards of communication sanctity.
- An extensive physical network of consumer-facing “retail” outlets that touches everyone.
- A postmaster is one of few individuals whose attestation of identity the government will accept in a passport application.
- A powerful local and understood global brand connoting independence, neutrality, and disinterest for each national post office.
- An [existing global federation](#) committed to world-wide service standards that tie together all four corners of the world.

Most people understandably do not think of the post office in these terms. But it is an unarguably potent mix of rights, infrastructures, capabilities,

<sup>2</sup> For more detail, see [Toward a Digital Trust Framework](#).

<sup>3</sup> A Crown corporation is a private business that exists by statute and whose only shareholder is the Crown (i.e., the State).

and relationships that could and is being retasked to address the demands of the digital environment.

These assets, let alone evolving capabilities such as [electronic courier](#), [electronic bill presentment and payment](#), and [electronic postmarking](#), can be augmented by acquired or partnered capabilities (e.g., commodity IT and security services) to address the full complement of structural pillars presented in Figure B. Only *Responsibility* is not immediately resolved to the degree that may be necessary.<sup>4</sup> Regardless, the postal administration represents an excellent TTP to facilitate the trust framework and perhaps even an identity management system. Were a risk-management program used to facilitate acceptance of greater liability and brought to market along with the other post office value-add, the digital trust framework is better than halfway made and digital identity in the public domain has one less obstacle to overcome.

Ultimately trust in the digital world will have to be borrowed from elsewhere – at best only to seed, at worst to persist. The world’s organization of national postal administrations is the ideal TTP to provide the needed assets.

XXX

This paper is available online at  
[http://www3.sympatico.ca/trdgrayson/recursive\\_content\\_id.html](http://www3.sympatico.ca/trdgrayson/recursive_content_id.html)

*Timothy Grayson is part of the eBusiness group at Canada Post Corporation, in Ottawa. He is an [essayist](#) and the author*

---

<sup>4</sup> Governments and post offices typically limit liability quite strictly – in the case of government to the point of “completely” and post offices to a standard typical of the delivery trade (e.g., cost of the service). We say “may be necessary” because there is inadequate proof to support the contention that the market will *insist* upon the TTP accepting broad transactional liability.

of *"Every Canadian's Guide to Common Contracts,"*  
published by HarperCollins.

[timothy.grayson@canadapost.ca](mailto:timothy.grayson@canadapost.ca)

©2003, Timothy Grayson. All rights reserved.