EVOLUTION OF THE ONLINE TRUST-MARK

by

Timothy R.D. Grayson

A trust mark is, loosely defined, any symbol or sign that represents an assurance of some understood message. A mark of trust can be a diploma hanging on a professional's wall; it could be a brand logo or name connoting certain expectations. The meaning of some markings, such as those above, inheres in the party directly: the doctor or the lodging. Other marks, such as the Good Housekeeping "Seal of Approval" or even the "Intel Inside" logo, extend the meaning to *derive* trust. In this latter form, a third party provides the assurance; its reliability is implicit in the assurance. Thus can a third-party arbiter add certainty to a transaction by attesting to actions and trustworthiness among the primary parties.

The Internet and the evolution of trust

The graphic browser was a radical shift from what the academics and government researchers primarily using the Internet had intended. By 1994, when shopping and advertising began their assault on the Web, the Internet was on its way to being the new communications paradigm among both academic colleagues and the common folk alike. The closed atmosphere of academia and the research community was on the run. Soon it would be impossible to distinguish who was at the other end of the communication, their credentials, or why they were there.

In 1994, advertising banners also began appearing on content-based Websites. The allegedly sustainable business model was to generate high traffic to a Site and increase advertising rates. This model, combined with an accelerating volume of viewers, created a "land grab" mentality online. For all else, this frontier period, was marked by almost perfect anonymity. Because no cash was exchanged between a Website and an online user, there was little need to identify one another. Change would come soon.

The catalyst for a stronger means of identifying parties in a transaction was e-commerce. Although the first online shopping malls also appeared in 1994, practical e-commerce arrived in 1995-96. In addition to a few early-adopting, better known retailers, thousands of unknown vendors came online selling to the world at large. Among them in this fiercely anonymous world were countless charlatans. Late Internet adopters retreated from e-commerce. Too many stories about credit card numbers being intercepted online and accounts decimated all but eliminated any trust for the medium and the recipients of their money.

The Internet industry responded decisively to the problem. First, information in transit would be protected by ever-stronger encryption technology. Second, Websites were encouraged to undergo independent authentication and business audits to validate that they were above-board and trustworthy. While these solutions were vastly different in intent and implementation, their outward appearance was similar: a seal or mark to indicate an independently validated trustworthiness. These initiatives marked the advent of the specific online "trust mark."

These trust marks were actually preceded by other casual marks of trust. They did not, however, provide any real assurance of security, privacy, or even trustworthiness. They arose out of e-commerce as retailers affixed the logos of major credit cards prominently on Web pages. The credit card logo was displayed to imply that a well-known, major company had adequate knowledge of and faith in the retailer's legitimacy to grant a merchant account. Much abused, it was eventually not enough for most consumers and served to direct effort toward more valuable signs and symbols.

Soon, other trust marks would extend the degree of Website validation on the consumer's behalf.

Some were associated with technology providers who assured Website security. The best examples of these seals are the logo marks of security technology firms (e.g., *Verisign*, *Baltimore*, and *Entrust*). Other marks focused on business attestation rather than specific technical security; they covered privacy, authenticity, business practices, etc. Typically they were the outcroppings of existing off-line symbols, although Internet-specific brands also developed. The most successful new organization was *TRUSTe*, which conducted audits and provided a seal for those entities that passed its scrutiny. The migrated version of the *Better Business Bureau's* seal of approval was a prominent example of an organization's existing reputation – for impartiality and consumer advocacy – being successfully applied on the Web. A third significant trust mark solution to this Internet trust deficit was the *WebTrust* seal granted by *The American Institute of Certified Public Accountants* and the *Canadian Institute of Chartered Accountants.* This seal could only be acquired after a thorough independent technology and business audit. In each case, the result was a visual manifestation of derived trust based on the logic that, "You, the consumer, know and can trust us, the third party auditor. We say the Website is trustworthy, so you can feel alright doing business with it."

The critical consistency and limitation of these early online trust marks was that they were directed one way: from merchant toward consumer/user. It was presumed that because the merchant was financially protected, having charged the credit card prior to completing the transaction, there was no need to identify or authenticate the trustworthiness of the consumer.

At the same time in the late 1990s, Web-based business-to-business transactions were gaining ground through exchanges and direct e-commerce activity. The Web was expected to become a less expensive, more inclusive replacement for existing EDI structures. In addition to reducing the data transport cost, using the Web would democratize B2B activity by making it easy for any and all vendors to do business with any buyer. The trust issues that arose again included credibility and trustworthiness at a distance. In this context, however, the burden of proving identity is on the party seeking access. Peer to peer (P2P) activity, such as eBay, created an even more pointed need to ensure participants' identities. Nobody knows anybody else; anybody could be somebody other than what they claim to be. Because eBay had no intent of policing user activity, contextual solutions self-organized. An un-moderated, participant rating scheme created a peer-controlled "live-and-die-by-reputation" environment. Another result was a payment system (*Pay-Pal*) that institutionalized part of the trust required between parties. Both of these solutions created trust marks of a sort. A star rating system made each participant known to others by his/her peer-generated rating, and the presence of the *Pay-Pal* symbol indicated a marginally protective process.

By the end of the 1990s, governments recognized the cost-effectiveness of connecting with citizens via Internet. Identity authentication in this context is relatively straightforward. The citizen knows the government and may be intuitively aware that of anyone, a government has the power to ensure that it is represented honestly online. Moreover, the government knows and shares personal information by which to make a sure connection between itself and the citizen. The marks of trust, therefore, are derived offline in the physical existence of government institutions and buildings, and the knowledge of government presence online.

Trust and the future of the Internet

Essential forms of trust absent in the early commercial development of the Internet were addressed *ad hoc* as need arose. The evolution of trust is ongoing, however, and corresponds to the increasing sophistication of the medium and its users. Thus far, the primary challenge addressed by a trust mark was the identification of trustworthy businesses. Today the trust mark is evolving to address three urgencies: a glaring trust deficit in user authentication; reaching the mass market with a sure means to validate and verify Web activity integrity; and a means of adding certainty to the transactional history of a Web-based interaction.

A relatively sophisticated online population and an established means of identifying the vendor has shifted the focus of trust assurance to the user. Rather than a business needing to prove to potential customers that it is legitimate and trustworthy, the consumer needs to prove him/herself. A primary driving force is identity theft and fraud. Billions of dollars disappear annually from the economy due to this misappropriation of commerce. Given these increasing losses, it's only a matter of time before a mark of authenticity will be required of the individual. But what will that trust mark look like?

A virtual identity needs to be attached to a real person or other entity in a trustworthy manner. Some of the shortcomings, however, are the constraint of standardization and a means to visually and machine-readably identify individuals with appropriate credentials. The absence of a definitive means of authenticating individuals will perpetuate identity theft and fraud. In turn, expansion of the Internet channel will be slowed until trust is injected into the system.

If we assume that all participants can be suitably authenticated, still the need to enhance trust in the total integrity of Internet activity remains. Regardless of whether the transaction is a financial one (e.g., a purchase) or the transfer of information (email and/or form), for many reasons we don't believe or trust the system. Even with high-quality, secure socket layer (SSL) security, there is no definitive assurance that any action happened as we believe. Presently the integrity of the transmission and the communication can be readily impeached.

A technological means and a mediating party that can attest to the veracity of an action across technology platforms and clients, application types, and even international boundaries is essential. The technical solution may be difficult to address but is not insurmountable given increasing standardization. Policy and legislative issues that are sure to arise will be abundantly more troublesome. Among other things, it will require negotiation among technology vendors and users of various sizes, governing legal frameworks, and notions of what integrity means. Requisite assumption of liability by that mediating party will further constrain those who would participate. Moreover, a universal standardizing body would have to implement the solution so that the resulting mark would be of equal value the world over.

As usual, the potential saviors bringing solutions to market are legion. There are few barriers to any organizations that can imagine, develop, and market a software solution. Among certain publics, a relatively accepting environment exists for some of these organizations to attest to transaction integrity as a trusted third party. What is glaringly absent in most of these instances, however, is a legal enforcement framework. Which is to say that the attestation is of limited value beyond psychic well being. Nowhere will this be more obvious than in non-repudiation services, an area where a trust mark will be most highly prized.

Transaction non-repudiation involves not only an attestation to identity and transaction integrity, but also life-cycle management. Stronger recourse for non-repudiation arbitration is a necessary condition for less trivial Web transactions, particularly large dollar volume, multi-party, and multiple-iteration transactions to gain serious acceptance. The essence of non-repudiation is to remove the ability for a party to deny any part or an entire transaction. A few crucial, discrete functions are required of the technology and processes. First, all parties must be strongly authenticated and identified throughout the process as rightful to the transaction. Second, the time and content of all communications must be recorded and archived. This creates a "paper trail," and while the recorded content is not an exact copy, each cryptographic profile would be unique and unmistakable. Finally, the independent party providing the non-repudiation service must maintain records through the required archival period. As with all other trust services, the non-repudiation service must manifest itself in a readily identifiable and unforgeable manner.

Summary

It has become evident that trust marks are an essential part of the Internet's evolution. However they must continue to evolve to provide the necessary trust in areas not yet resolved, including: user authentication; validation and verification of web activity integrity; and the addition of certainty to web transaction activity. An online, non-repudiable trust mark will address these issues and help provide the necessary solution.

Timothy Grayson works for Canada Post Corporation, in Ottawa. He is the author of Every Canadian's Guide to Common Contracts *published by HarperCollins. He can be contacted at timothy.grayson@canadapost.ca*