Abstract
This paper reports on a longitudinal interpretive case study of the Financial Services Technology Consortium eCheck project, and the failed attempts to promote eCheck and an enabling technology, FSML, as vertical IT standards. Based on interviews and archival data, a series of linked technical decisions are examined, covering a seven-year period. Early technical decisions put the design team's work on a technical trajectory, which they chose not to abandon, contributing to the failure of these proposed standards. We discuss the evidence in light of technology evolution theory and offer suggestions for future research on vertical standards setting.

Keywords: technology evolution, path dependence, IT standards

INTRODUCTION
IT standards are important facilitators for e-commerce; vertical IT standards support commerce in specific industries. The longitudinal case study reported here examines an effort to design and promote two vertical IT standards for banking: the Financial Services Markup Language (FSML) and eCheck, an FSML-based payment mechanism. We analyse these e-payments standards initiatives in light of technology evolution theory.

Data were gathered as part of a longitudinal interpretive case study of an initiative begun in 1994 and sponsored by the Financial Services Technology Consortium to design a general-purpose electronic payment mechanism, eCheck. However, efforts to promote eCheck and FSML as standards were not successful. This paper addresses the questions: Why, with many influential companies behind it, and with strong technical expertise on the development team, did eCheck and FSML fail to take hold as standards? What do these findings imply for future standards-setting efforts?

The paper is organized as follows. We define vertical IT standards, review the standard-setting literature and explain the application of technology evolution theory to standard setting. The study methodology is described, followed by a brief history of key events and decisions in the FSTC eCheck project. Consistent with technology evolution theory, we provide evidence of one aspect that contributed to the failure of FSML and eCheck: an ineffective response to path dependency. A series of interconnected technical decisions (regarding hardware, security mechanisms and coding considerations) set the development team onto an ill-fated technical trajectory and they did not change course in time to avoid failure. We discuss the implications for participants in standard-setting processes and offer suggestions for further research.

IT STANDARDS: DEFINITIONS AND VARIATIONS
Aggarwal and Walden (2003) define an IT standard as 'a set of technical specifications that allow communication between IT entities' (similar definitions are offered by David and Greenstein 1990; Garud and Kumaraswamy 1995; Gosain 2003). A vertical standard aims at one
industry, while a horizontal standard is applicable across a variety of industries. Vertical IT standard-setting processes have been under-studied (Jain and Zhao 2003 and Markus et al. 2003). This paper analyses the design and failed promotion of two vertical IT standards for banking: FSML and eCheck. eCheck can be seen as an ‘architecture of related standards’ (West and Dedrick 2000), in that its design encompassed several related technologies.

FSTC members attempted to establish FSML as a standard and eCheck as a de facto standard. The act of ratification by a standards-development organization (SDO) or governmental institution is the criterion for designation as a de jure standard. Although SDOs do not always include all relevant stakeholders, inclusion is considered a requirement of a de jure process (Chiesa et al. 2002). A de facto standard is established through widespread adoption and use, without de jure ratification (Gallaugher and Wang 2002). Many studies invoke Anderson and Tushman’s (1990) criterion – it is a de facto standard if 50% of the market adopts it. The line between de jure and de facto is not crisply drawn; industry organizations sometimes promote adoption of de facto standards (Graham et al. 2003). The eCheck Project involved a de jure standard-setting process since membership in FSTC was open to any financial industry participant (inclusion criterion) and since FSML was formally proposed to the World Wide Web Consortium (W3C). However, it was never ratified, and neither FSML nor eCheck took hold as de facto standards, since they fell far short of achieving a 50% market share.

This paper examines how specific design decisions contributed to the failure of FSML to become a standard for the secure transmission of financial documents, which in turn, impeded attempts to establish eCheck as a standard payment mechanism. Technology evolution theory is used to examine both social factors and technical choices, consistent with recent calls for IS researchers to focus on the IT artefact (Benbasat and Zmud 2003; Orlikowski and Iacono 2001), and organizational researchers’ admonition to focus on how ‘material objects … (including computer and network technologies) enable and constrain actors’ (Greener 2002).

TECHNOLOGY EVOLUTION THEORY

Technology evolution theory posits that, over time, standards are shaped by evolutionary processes, including interaction between the technology and a broader social system and the effects of punctuating events. Abernathy and Clark (1985: 4) observed that ‘some innovations disrupt, destroy and make obsolete established competence’ within companies and industries (see also Abernathy and Utterback 1978). Echoing Abernathy et al., Tushman and Anderson (1986: 439) proposed that ‘technology evolves through periods of incremental change punctuated by technological breakthroughs that either enhance or destroy the competence of firms in an industry.’ Competence-destroying technologies create challenges for incumbents, who have to acquire new knowledge and skill and make changes to the systems and processes that support older technologies (the concept of a competence-destroying technology is a precursor to that of disruptive technology, advanced by Bower and Christensen 1995 and Christensen 1997). Anderson and Tushman (1990) note the relationship between technology evolution and standard setting: a technical breakthrough ushers in a period of intense competition among technologies, applications, and potential standards, until a standard eventually appears. During this period, organizations may resist change for a variety of reasons, including organizational inertia and interlocking interests. Others propose that these factors are less influential than network externalities (‘wider acceptance of the technology increases its usefulness’) and uncertainty about the future performance of a new technology (Loch and Huberman 1999: 163).

A branch of technology evolution theory posits that ongoing technology usage is heavily influenced by early technology adoption choices, which (in combination with organizational structures and processes) put powerful constraints on subsequent choices (see, for example, the discussion of the persistence of the QWERTY keyboard despite the superiority of the Dvorak keyboard in Wilsford 1994. See also Arthur 1989, 1990; David 1985). This phenomenon is called ‘path dependence’. A recent study of the web services standards setting process reports that IT standards sometimes ‘force adopters into specific trajectories of technology use’ (Gosain 2003: 11). Participants in the standards-setting process operate with incomplete information and face uncertainty about such aspects as: Will this bundle of technologies work as planned? Will better technologies emerge before we have harvested value from this technology? Will a dominant player set a de facto standard? Gosain contends that each decision in the standards-setting process creates dependencies which constrain future action; he calls these ‘inter-temporal dependencies’. Hereafter, we will use the term ‘path dependency’.

The path dependence explanation has been criticized as overly deterministic. Greener (2002: 618) contends: ‘Path-dependency provides us with a compelling description of how history comes to be embedded within organizations, but is inadequate in explaining exactly how this comes to happen.’ Drawing on actor-network theory, Greener proposes that three factors influence whether organizations remain stuck in or break out of path dependence: material properties of objects, simplification and boundary roles. Objects (including traditional objects such as buildings, industrial equipment and documents, as well as information and
communication technologies) matter, according to Greener, because of the capital invested in them as well as the structures and functions that surround them. He calls for further examination of how organizational objects impede change. Simplification refers to the mechanisms that individuals and organizations use to reduce the perceived complexity that accompanies extensive market choices (and high levels of information overload). So, for example, a firm might designate certain products as internal standards (e.g., designating Microsoft Office as the standard desktop environment). While objects and simplification tend to reinforce path dependence, boundary roles can help organizations break out of path dependence, according to Greener. Actors on the boundaries (within and across organizations) have access to ideas that can challenge the status quo, some of these actors have the ability to translate new ideas into terminology that allows the new ideas or new practices to be accepted by organizational members.

To summarize, technology evolution theory specifies the importance of punctuating events (technological discontinuities) and variation in the adaptability of participants in a particular industry ecosystem. IT standards are subject to path dependencies because early technical decisions, made based on incomplete information, raise switching costs (due to the investments in IT objects and associated processes and structures, as well as simplification strategies). It has been asserted that path dependence can be overcome with recognition of the constraining properties of objects and simplification measures, combined with policies and incentives that encourage actors in boundary roles.

Technology evolution theory leads to our overall research questions: During the FSML/eCheck standard-setting process, did specific technical choices lead to path dependency? If so, did participants allow the project to be trapped by path dependency, or did they attempt to overcome it?

METHODOLOGY

The FSTC eCheck project was launched in spring 1994; this study began in 1996, using an interpretive methodology (Klein and Meyers 1999), as part of a larger multi-case study to examine opportunities and risks of e-commerce on the Internet. Face-to-face interviews of one to three hours each were conducted with the eCheck project manager and two members of the eCheck design team: a representative from a bank’s emerging technologies group and a researcher from an IT vendor organization. The first phase of our study examined events and issues as the 27-member eCheck team refined the design, assessed its potential business value and considered how to conduct a pilot test. Interviews were taped, professionally transcribed and then analysed along with project memos, reports, and presentations, to develop a chronology of events and decisions to that point. A prepared case history (Gelinas and Gogan 1997) was reviewed by interviewees and they confirmed that it accurately represented the events and issues.

In Fall 1997 plans for a pilot test were announced (Clark 1997): the US Air Force would pay some vendors via eCheck, with the assistance of the United States Treasury. To learn about this phase of the project semi-structured interviews (one to four hours each) were conducted with seven people, representing FSTC, two commercial banks, the Federal Reserve Bank, the government and software vendors. Informants reflected on business and technical challenges in the pilot project. All but one of these interviews were taped and transcribed. Archival sources (team memos, reports and presentations) and public-source documents (press releases, articles) were again gathered and two new case histories were prepared – one with a technical focus (Gelinas et al. 2003) and one with a project focus (Gogan et al. 2004) – and given to interviewees to review. Based on their clarifications (and triangulating against interview and archival data) we made minor corrections to the cases. In 2003, follow-up interviews were conducted with four key eCheck project participants.

To analyse the FSML/eCheck standards development process, we extracted those interview segments and archival data (from data collected 1996–2003) which addressed technical design considerations and standards-setting discussions and events. From these a timeline of technical and business decisions related to the standardization process was constructed.

FINDINGS: ECHECK PROJECT OVERVIEW

The Financial Services Technology Consortium was formed in 1993 to sponsor ‘non-competitive collaborative research and development on inter-bank technical projects affecting the entire financial services industry’ (www.fstc.org [as of 1996]). Any US-based bank paying the $15,000 annual fee could participate as a Principal. At the time, 12 US-based financial institutions were Principals: Bank One, Bank of America, Bank Boston, Barnett Bank, Cardinal Bank Shares, Chase Manhattan, Citibank, Corestates, Glenview State Bank, Huntington Bank, Nations Bank, and Wells Fargo. So membership included the largest US banks (such as Citibank and Chase Manhattan) as well as smaller banks (such as Barnett and Glenview State). Banking industry IT vendors participated as Associates and non-profit or governmental entities participated as Advisory Members. The eCheck project, launched in Spring 1994, was one of several FSTC projects. The 27 organizations represented on the eCheck design team (seven banks, 13 vendors, seven advisory members; see Figure 1) each put
up $150,000 (or equivalent personnel) to participate in the design phase. Most eCheck team members were technical employees, many (including the project lead) were from the emerging technologies group in their organizations. Around 1995 or 1996, the project manager expected that several pilot tests would be conducted, in different e-commerce settings. However, the FSTC Board of Directors (who were higher-level managers in banks) approved just one pilot test (with the US Treasury and Department of Defense). In 1997, when the project moved into the pilot phase, the price rose to $500,000 per participant and the team shrank to 12 organizations: two commercial banks, seven IT vendors, US Treasury, US DoD and the Federal Reserve Bank of Boston.

Bankers who joined FSTC and participated in the eCheck Project were motivated both by a desire to expand their business domain and to defend it against traditional competitors and non-bank competitors. Some in the banking industry at that time envisioned ways to make money from a new payment infrastructure, while many felt threatened. Banks had made significant investments in traditional paper cheque clearing and lockbox services, and worried that competence-destroying technologies would threaten these services. They also worried about non-bank rivals, according to a news item at the time: ‘FSTC is scrambling to define the electronic-information infrastructure before such potential rivals as Microsoft, MasterCard International, Visa International and Internet navigator Netscape do it for (and to) them’ (Teitelman 1995: 21).

A public proof-of-concept demonstration of the eCheck design was held in Fall 1996, followed by two more years of design work, project planning and negotiations over intellectual property and other issues, before the first eCheck was sent, in summer 1998. For three years, eCheck continued to be tested (in two different configurations – one in which commercial banks served as payer bank and payee bank, and one (after the commercial banks withdrew from the project) with the Federal Reserve Bank serving as the payer’s bank (for details, see Gogan et al. 2004). The US Treasury pilot test ended in July 2001.

Having introduced the eCheck project, we next describe the standard-setting process.

FINDINGS: FOUR KEY DECISIONS IN THE FSML/ECHECK STANDARDS–SETTING PROCESS

Technical and policy design choices can create path dependency in a standards-setting process. Path dependency in the eCheck project came from four early design decisions. An eCheck would:
1. be a digitally signed ‘writing’;
2. use public-key infrastructure (PKI);
3. use two-factor token-based authentication; and
4. code the eCheckbook using a markup language.

Decision 1: A digitally-signed writing

Since paper cheques were the dominant form of non-cash financial transactions in the US, the team hoped that an electronic equivalent would ‘be readily accepted by the marketplace’ (FSTC 1995). In a 1994 meeting, a spokesman from the National Security Agency discussed a privacy-enhanced email system, which utilized a PCMCIA card to hold encryption keys. Milt Anderson, an FSTC member and cryptography expert from Bellcore, felt this idea would fit well with legal definitions of cheques. He recalled: ‘A [paper] cheque is legally defined as a signed “writing”, containing certain prescribed pieces of information. A “writing” is similar to a “message”. I thought: this will be easy. A cheque is a message that carries financial information – like date, pay-to-the-order of and a few other things. We would develop an electronic “writing”, equivalent to the manual version, but cryptographically signed, using the technology of privacy-enhanced e-mail.’

Some participants in this effort agreed that an electronic cheque should be designed to conform as much as possible to existing laws, regulations and payment-clearing operations. A few participants argued that an electronic equivalent of a paper cheque was an example of being ‘stuck in a conventional paradigm’, but most members liked the idea that banks could leverage their existing processing and regulatory infrastructures. A team member from the Boston Fed stated, ‘We basically married eCheck to paper cheque law. It just made more sense’. It was further argued that a
well-designed eCheck could include extensions that make it operate like a lockbox, certified cheque or any number of flexible variants. So, despite some controversy, most participants felt the choice to design eCheck as an electronic ‘writing’ was a smart move.

Decision 2: PKI

To be valid, a conventional paper cheque must be signed. Once it was agreed that eCheck would be a form of privacy-enhanced email, some security experts proposed the use of public-key infrastructure (PKI), which relies on digital certificates and public/private key encryption to produce and verify a digital signature. The security experts argued (FSTC 1995: 8): ‘Public key cryptographic signatures are necessary because the signature of each signer, computed using the signer’s private key, can be verified by anyone else who knows the signer’s public key. This property is not shared by (systems that use) secret-key cryptography.’ In PKI, digital certificates are issued from trusted certificate authorities. The eCheck team had many discussions regarding who should serve as certificate authorities. They ultimately chose to utilize two levels of certificate authorities: the US Treasury served as CA for the banks and each bank served as a CA for its customers. It took a long time to reach this decision, because some members had concerns about certificate issuance and revocation (Was it appropriate for Treasury to certify banks, or should a different party take this role? Was it appropriate for banks to issue certificates for their own customers or would it be better for a non-bank party to serve in that role? How would certificate revocation be handled and controlled?). Also bankers were concerned about liability issues. A banker asked ‘Are we accepting new liability by enabling a third party to determine that this item is validly signed?’ A decision was made that a bank’s certificate would indicate not an account-holder’s identity, per se, but rather that the certificate would link the digital signature with a particular account. A banker summed up this approach: ‘I’m not giving someone a certificate that says they are John Doe; I’m giving someone a certificate that says this signature was authorized on this account at the time that it was given out.’ Once that issue was resolved, team members agreed to the use of PKI.

Decision 3: Two-factor, token-based authentication

The decision to utilize PKI led to a hardware decision. Security experts on the design team (including representatives from Bellcore, IBM, IRE and BBN) strongly urged that eCheck utilize a separate ‘token’ to store the necessary cryptographic private keys. A security token is a simple hardware device – such as a smart card or key fob – that can be used in conjunction with another hardware device. The design team chose to place the cryptographic keys on a smart card. To apply a digital signature to an eCheck prior to sending it to its recipient, a payer would insert the card into a reader on or attached to their computer. This two-factor authentication process (I have a token and I know a password), combined with digital signatures, provides optimal security.

At various times FSTC members questioned whether a token was really necessary; this was the subject of many rounds of discussions, including at the proof-of-concept demonstration in Fall 1996, when it was the subject of extensive discussion. The project leader at that time explained that it was easier to protect security on a card than on the Internet itself: ‘If this system is successful, it will handle trillions of dollars of transactions, so we cannot compromise on security. By putting the certificates on an offline device, we’re removing the security challenge from the network … . The basic idea is to protect those keys from being compromised in any way … . Plus, people are used to carrying cards. This is portable and safe.’

During deliberations in 1995, some members expressed discomfort with the cost of a separate card reader, this factor influenced the team’s decision. A representative from IBM stated that virtually all PCs would be equipped with PCMCIA slots by 1998. As it happens, however, most computer manufacturers did not include a PCMCIA slot on their desktop models. Laptops, which were equipped with PCMCIA slots by 1998, today use smaller USB ports instead.

Decision 4: Use of a markup language

Standardized Generalized Markup Language (SGML) is a set of specifications for creating a markup language (HTML is a markup language that is defined by SGML). The eCheck designers wanted to use a markup language because ‘this will make it easy for developers of electronic commerce software to integrate electronic checks into their products, and it will encourage early adoption. A humanly readable format is also easier to debug … ’ (Anderson 1996: 16). Other coding languages were considered, but the team liked that SGML was an ISO standard (ISO 8879). In choosing how to utilize SGML, the team wanted to minimize code complexity and maximize efficiency. This latter concern derived from the earlier decision to use PCMCIA cards, which had limited capacity.

In 1995, when the team first began to consider how to use a markup language to structure eCheck documents, no markup language had as yet been designed that could accommodate digital signatures. So, the team developed the Financial Services Markup Language.
FSML was designed for financial applications only, and eCheck would be the first application of it. Milt Anderson (1996) explained: ‘The simplicity of FSML makes it compatible with the memory, processing, and interface speed limitations of smart cards.’

Development of FSML made it possible for the team to design eCheck with a modular block structure, with cryptographic functions separated from check writing/endorsing functions ‘to facilitate applications of this cryptographic infrastructure to secure other financial instruments or documents.’ (FSTC 1995: 7). So, a variety of documents could be attached to eCheck, and new functionality could easily be added to the core, without creating a maintenance nightmare. The designers were very pleased with the flexibility that FSML provided. Figure 2 depicts the block structure design of the eCheckbook.

The eCheck system architecture at two points in time during the pilot test is described in Gelinas et al. (2003), space does not permit a full description here. At first, a ‘four-corner’ model was used, with participation by two commercial banks, serving as payers’ and payees’ banks as would normally be the case in financial transactions. The second architecture, adopted when these two banks withdrew from the project, placed the Federal Reserve in the role of the payer’s bank. Of the four design decisions described above, only the decision to utilize PKI was affected by this system architecture change (because now the Treasury acted as a root certificate authority for the Federal Reserve Bank). One participating banker revealed that his banks’ views on PKI played a part in their withdrawal from the pilot. Review of our interviews fails to reveal whether the other bank took issue with the use of PKI at that time. In any case, the pilot test was able to continue, with the US Treasury serving as a root authority.

To summarize the evolution of design choices related to FSML: A cheque is a ‘signed writing’, so an eCheck would be a digitally signed promise to pay. The design team chose PKI and token-based two-factor authentication. On the assumption that they would soon be ubiquitous, PCMCIA cards were the token of choice. It was felt that a markup language was the best way to code the eCheck, but no available markup language could handle digital signatures. To support digital signatures and fit the memory limitations of PCMCIA cards, a decision was made to create FSML. As the saying goes, one thing led to another. Unfortunately, these decisions, although thoroughly discussed and thought, by the core eCheck team, to constitute reasonable solutions to specific challenges, set the project on a technical trajectory that would prove problematic as other developments unfolded. We discuss these developments next.

**OBSTACLES ON THE PATH TO SUCCESSFUL STANDARDIZATION**

The eCheck design effort began in 1994 and the pilot test was launched in Fall 1997. At that time, the eCheck team shrunk from the 27 initial members to 12 members who raised the funding level to $500,000 each to participate in the pilot test phase (some of the IT vendors spent considerably more than $500,000). According to the project manager, some early participants who chose not to go on to this next phase were
In June 1998 the first eCheck payment of the US Treasury pilot test was made, and in September the W3C published the specifications for FSML for public review. In 1999 the SDML specifications were posted for review (www.w3.org/TR/NOTE-SDML), neither FSML nor SDML were ever formally ratified. Had it been clear to the eCheck team in 1995 that XML would become a standard, they might have considered working within the XML framework instead of designing an industry-customized markup language. Still, even today, eCheck design team participants insist that FSML/SDML was an excellent fit for the eCheck application. Chuck Wade, the team member who represented BBN (later, GTE Internetworking), explained that most SGML-derived markup languages, including XML, inherit a language flaw: all internal names (e.g., variables) are defined as ‘global’, meaning that the same name must be unique throughout a document. When two documents are combined into a new document (such as when a recipient adds a digital certificate to endorse an eCheck), then name ‘collisions’ must be resolved by defining replacement names that will be unique in the combined document. Once a document has been digitally signed, names cannot be redefined, since any change to a document would invalidate the digital signature. In FSML this problem is resolved by defining name scoping rules (similar to the way many computer languages work): an FSML name is unique only within the subdocument that contains it. XML lacked this feature at that time, and then the group working on XML did not see this as an important shortcoming, according to Wade. In the April 1998 SDML announcement, FSTC was defending the sub-document naming approach in FSML and SDML. Later, at least one FSTC representative did join an IETF/W3C joint working group (XML DSig) to work on ways to digitally sign XML documents and in Fall 1999 FSTC announced that it intended to develop FSML Version 2.0 using XML (Anderson 1996: 18). This effort petered out as participants became involved in other initiatives.

In 1999 and 2000 eCheck’s designers continued to believe that two-factor, token-based authentication offered the best security for Internet-based payments. A representative from the Boston Fed stated: ‘The last thing the Federal Reserve wanted was to end up on the front page of the Wall Street Journal saying, “Fed implements new payment system and millions of dollars came out of the network and got lost.” Using PKI on a smart card helped prevent that.’ The choice of a PCMCIA card had made it necessary to design a markup language that could fit the constraints of this token, which led FSTC to design FSML. At first, XML was not on anyone’s radar screen. Then, when team members became aware of it, they viewed it as inappropriate because of its global naming property. In 1998 they tried to promote FSML as an alternative to XML, but in 1999 they seem to have decided ‘if we can’t beat them, let’s join them.’ Possibly at that point they were hoping that another pilot test could be conducted. However, by then various mergers and acquisitions, as well as preparations for year 2000, had led to changes in banks’ priorities. No more pilot tests were done on eCheck.

During a February 1999 presentation, one banker reported that the decision to use PKI was a ‘barrier’ to success in the eCheck project. During testing of the system in the months prior to the first eCheck payment, many problems had cropped up – ‘a lot of problems with all of these digital certificates,’ said this informant. ‘This technology was not ready for prime time.’ Had the team decided not to utilize PKI, they would have avoided the headaches of certificate issuance and revocation. Note that subsequently, both of the banks that participated in
eCheck were acquired by Bank of America, an FSTC member that had not participated in the eCheck project. Bank of America is one of the founding institutions of another PKI initiative, Identrus. Identrus participants also include Barclays, Chase Manhattan, Citigroup and other major banking institutions (another bank, which had been one of the 27 members of the initial design team but dropped out at the pilot stage, also joined the Identrus initiative). Today, the American Banking Association endorses Identrus (see www.aba.com/About+ABA/_TECH_digsigs.htm). So, the choice of PKI, per se, should not be seen as the cause of eCheck’s failure.

The US Treasury pilot test officially ended in July 2001 and no more pilot tests were conducted on this technology; eCheck itself is officially ‘dead’. The US Treasury did go on to test other approaches to B2B payments and some pieces of eCheck found their way into those tests. As of 2005, there is still no clear winner in the B2B payments arena with FSTC continuing to sponsor various R&D projects. A few for-profit companies licensed the eCheck technology, but utilized only portions of it: Xign Corporation uses some eCheck technology for its Order To Pay service and they also offer a smart card option. PayMode, developed by Clareon (which is now owned by Bank of America) retains some eCheck-like functionality. However, its processing architecture is quite different, it does not use tokens, and it does use XML.

In 2003, follow-up interviews were held with several participants. One informant questioned whether ‘there is enough value in the digital signature to be worth the pain’. The project manager noted: ‘We never did a separate business case regarding whether the hardware token was justified.’ Still, he and others gave no indication that the core eCheck team ever seriously reconsidered the four key design choices during the Treasury pilot test. The project manager felt the key shortcoming of the project was inadequate attention to marketing, both to the broader FSTC membership and to external parties. He also observed that the eCheck project was but one of many ill-fated payment-standards initiatives in the late nineties. For example, MasterCard and Visa collaborated on the SET standard for secure online credit-card payments, and, despite spending huge amounts to promote SET it was a failure in the US.

An informant from the US Treasury reflected on lessons learned, both from observing the failure of SET and participating in the attempt to develop and promote FSML: ‘Number one, you can’t bet on a standard. You don’t know what standards will ultimately win out. So, you can’t make a huge investment with emerging standards … You really need some competition among various projects to find out which is the best, which one can become a standard … So, for those reasons and others, we now definitely go toward limited, small, achievable implementations. We don’t like the Big Bang approach. We don’t bet that a standard will work.’ He added ‘even though eCheck did not succeed, we learned a great deal from that effort.’

Figure 3 summarizes the eCheck Project key decisions and related activities that affected the banking industry during the same years.

<table>
<thead>
<tr>
<th>FSTC eCheck activities/decisions</th>
<th>External Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1994 eCheck Project launched.</td>
<td></td>
</tr>
<tr>
<td>eCheck to be an electronic ‘writing’.</td>
<td></td>
</tr>
<tr>
<td>PKI and 2-factor, token-based authentication discussed.</td>
<td></td>
</tr>
<tr>
<td>Work on FSML starts, ahead of final decision about PKI.</td>
<td></td>
</tr>
<tr>
<td>1995 Proof-of concept demonstration in Fall, using early version of FSML, PKI and card.</td>
<td>Rapid growth in e-commerce.</td>
</tr>
<tr>
<td></td>
<td>Many dot-coms form.</td>
</tr>
<tr>
<td>1996 SDML development begins.</td>
<td>XML is introduced.</td>
</tr>
<tr>
<td>1997 Team shrinks form 27 to 12 organizations.</td>
<td>Banks start Y2K work.</td>
</tr>
<tr>
<td>Choice of PKI, FSML, card tokens finalized.</td>
<td>February: XML ratified by W3C Y2K a priority at most banks.</td>
</tr>
<tr>
<td>1998 April: SDML announced.</td>
<td></td>
</tr>
<tr>
<td>June: first eCheck payment in pilot test.</td>
<td></td>
</tr>
<tr>
<td>Sept.: W3C publishes FSML specs for public review.</td>
<td></td>
</tr>
<tr>
<td>1999 W3C publishes SDML specs for public review; FSTC states it will work on an XML-compliant version of FSML.</td>
<td>XML gains momentum.</td>
</tr>
<tr>
<td></td>
<td>Y2K a top priority at most banks.</td>
</tr>
<tr>
<td>2000 Some participants leave the pilot test, prompting shift from 4-corner to Z-flow design.</td>
<td>XML widely accepted.</td>
</tr>
<tr>
<td></td>
<td>Dot-com stocks crash in April.</td>
</tr>
<tr>
<td>FSML work apparently abandoned.</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3. Timeline: eCheck and related external events
DISCUSSION: CONTRIBUTIONS AND LIMITATIONS

Findings from a longitudinal study covering seven years cannot be fully captured in 8,000 words. We have contributed to the standards-setting literature and the theory of technology evolution by tracing four key decisions in the FSML standards development process. These early technical choices were tightly interlinked. Since a decision to change any of these elements would necessitate change in the others, there was pressure to stay the course, similar Gosain’s (2003) observations in his study of web services.

As discussed above, Greener (2002) proposed that objects, including information technologies, can create strong path dependence and this seems to have been the case in the eCheck project. At each step the eCheck team made reasonable technical choices, but in aggregate those choices put them on a technical trajectory that they found difficult to alter, even when circumstances warranted a change. In retrospect, it seems evident that the team should have reversed some of their earlier decisions. Had they decided not to utilize a hardware token, there would have been less of a need to design a specialized markup language (since the FSML decision was driven by the small capacity of card tokens at that time). The timing of the project was such that they probably would still not have initially made use of XML, which was developed in 1996, two years after the eCheck project began; that seems like a case of bad luck! They probably should have recognized earlier that XML would become widely accepted.

The team’s early commitment to PKI and PCMCIA cards were pivotal decisions that set the project onto the FSML path. Specific material properties of PKI, PCMCIA cards, and markup languages created incentives to stay the course and provided strong disincentives to change course. However, choices could have been made to go down different paths.

One of the participants from the US Treasury suggested that it might have been beneficial to support multiple, competing design paths simultaneously, in order to build in flexibility to the effort and acknowledge the uncertainty attendant with each choice. For example, the team might have said, ‘let’s explore one option that involves the use of PKI and another option that will not require PKI.’ Or, ‘let’s explore one option that utilizes token-based authentication and another that does not.’ A broadly representative consortium such as FSTC, with a mission to explore applicable technologies, could justify such an approach. So could an institution with the clout of the US Treasury. Indeed, at least one of the vendors participating in the eCheck project – IBM – does this on a regular basis, by participating on many different competing initiatives. However, each additional option that gets explored adds costs for the participants, and would also increase overall project complexity and time. Only an organization with deep pockets, a strong market position and the ability to be patient could comfortably adopt such a strategy. The smaller IT vendors, such as IRE and BBN, might have balked at such an approach.

Greener also suggests that boundary-spanning roles can help organizations break out of their path dependence. An option open to FSTC would have been to allocate more resources to boundary-spanning roles, by sending eCheck representatives to meetings of organizations such as the W3C or IETF early on, as well as making, as the eCheck project manager observed, more frequent updates to the broader FSTC membership, which included banks that had chosen not to participate in the eCheck effort. Perhaps then, eCheck participants would have recognized the significance of XML earlier and been able to change course on that issue, and perhaps the arguments against smart cards would have received greater consideration. It is also possible to envisage the situation where a senior person could have recognized that FSML was a vertical standard colliding with XML, a horizontal standard. If that person could have articulated the case for collaboration with the horizontal standard-setters, the project might have taken a different course.

We have provided persuasive evidence that path dependency may have contributed to the failure of eCheck or FSML to become standards, but we cannot claim that participants were forced to stay on the path they had chosen. Nor can we claim that path dependence tells the whole story. In the follow-up interviews, other suggestions as to why results fell short of expectations included: insufficient resources devoted to marketing (both within the participating organizations and to a broader constituency); distraction due to preparations for the Year 2000; wrong participants in key positions; and other factors (see also Gogan et al. 2006 for an analysis of the eCheck project based on theories derived from the literature of strategic alliances).

Ironically, a consortium is supposed to be a mechanism to help representatives from different organizations share ideas and introduce novel practices to each other. The eCheck team members may have received the cross-fertilization benefit early on, but as time went by, they seem to have jelled into their own organization, with a separate identity. Possibly their identification with the team may have led to an ‘us against them’ mentality and an unwillingness to accept new ideas from outside the team. If so, then encouragement of boundary roles was doubly important (and apparently lacking). Nickerson and zur Muehlen (2003) observed that technical participants’ beliefs and behaviours often align more with the culture of their technical profession than with that of the corporations which they represent. This identification with a technical culture may cause standards-setting participants to make design decisions that are sub-optimal for their companies, or lead participants to exit a standards-setting process rather
than compromise. It is quite possible that this phenomenon was inherent in the eCheck project. It is also possible that the particular cast of characters in this story was a group of very stubborn individuals who simply refused to accept that they had made some poor design choices. We do know that 13 members chose not to go beyond the design phase, but unfortunately we do not know their specific reasons. As noted above, we did not have an opportunity to interview those team members who opted out of the pilot-test phase; this is an important study limitation.

Therefore, this longitudinal case study paints a rich, but limited, picture of the trials and tribulations of standards setting. Future studies are needed to improve our understanding of this important process, as we discuss next.

SUGGESTIONS FOR FUTURE RESEARCH

Technology evolution theory emphasizes the role of technological discontinuities (or punctuations) and path dependency. Further close examination of the social interaction processes that influence IT standards would be beneficial, as suggested by Graham et al. (2003) who looked at a variety of B2B standards-setting initiatives, and Gosain (2003) who utilized social shaping theory (which suggests that technology is shaped by the social interactions of stakeholders; see also Mackenzie and Waczman 1999). Markus et al. (2003) observe that standard setting efforts often affect multiple stakeholder groups, with varying priorities and requirements, and De Vries et al. (2003: 92) observe that inadequate stakeholder representation can be problematic, especially in standards-setting processes that are sponsored by industry consortia (such as FSTC). They contend: ‘A major barrier appeared to be the lack of conscious and systematic stakeholder identification and selection prior to the standardization process, including determining whether participants bring adequate resources – such as time, money, expertise, and social influence – to these efforts.’ It is possible that poor stakeholder representation was a factor in the eCheck story, but unfortunately we were not able to gather data on team selection (other than being told that ‘any FSTC member was welcome to participate’). The project manager’s concern that insufficient attention was given to marketing (both within FSTC and to external constituents) suggests poor management of stakeholder concerns. This aspect deserves closer attention in future studies of vertical standard setting.

From the eCheck example, we can see that vertical IT standard-setting efforts can fall into a path-dependency trap, especially when specific IT choices are interdependent. Consistent with Greener, we find that material objects do contribute to path dependence. Further research is needed to uncover effective ways to overcome this path dependence – especially when vertical standards collide with horizontal standards. Thus, close examination of specific technical choices made during a standard-setting process, combined with close examination of the stakeholder views and social interactions that shape those choices will yield a clearer and more complete picture to guide the theory and practice of vertical IT standards development and to strengthen theories of technology evolution.

ACKNOWLEDGEMENTS

I am indebted to Ulric J. Gelinas, who was an equal and valuable partner in the eCheck project research but who opted out of this paper. Thanks also to the anonymous reviewers, for helpful comments. Portions of this work were supported by the Bentley College Invision Study, Jane Fedorowicz, Principal Investigator. Other Invision team members were Joe Gelinas, Lynne Markus, Amy Ray, Cathy Usoff and Chris Williams.

References


