Computer Networks 67 (2014) 235–251

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

# Banking on interoperability: Secure, interoperable credential management

Glenn Benson [a], Shiu-Kai Chin [b], Sean Croston [d,1], Karthick Jayaraman [c,*,2], Susan Older [b]

[a] JP Morgan Chase & Co., 270 Park Ave FL 12, New York, NY 10017, USA[3]
[b] Dept. of EECS, Syracuse University, Syracuse, NY 13244, USA
[c] Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA
[d] State Street Bank and Trust Company, 1 Lincoln St, Boston, MA 02111, USA

ARTICLE INFO

*Article history:*
Received 27 March 2012
Received in revised form 16 March 2014
Accepted 25 March 2014
Available online 1 April 2014

*Keywords:*
Certificate
Authentication
Authorization
Protocols
Trust
Wholesale banking

ABSTRACT

An interoperable credential system allows users to reference a single asymmetric key pair to logon to multiple web sites and digitally sign transactions. Models that govern how keys are created, authorized, validated, and revoked are a crucial part of such a system. These models have security, scalability, and liability implications for businesses, so the requirements vary depending on the parties involved. However, the prevailing the public key infrastructure (PKI) system does not meet these diverse needs. PKI requires a certificate authority (CA) to act as a trusted third party for the parties in a transaction. For example, PKI features a receiver key validation model that requires the receiver of the transaction to communicate with a CA to validate the sender's key used to sign a transaction. These aspects conflict with liability concerns and interoperability goals of businesses doing high-value transactions such as wholesale banking. This paper presents Partner Key Management (PKM) as a mechanism which sufficiently addresses security and liability concerns of businesses performing high-value online transactions, and uses wholesale banking as the motivating example. PKM does not rely on a trusted third party, and features several flexible revocation models to accommodate diverse regulations. PKM is not merely a proposal. Rather, the financial industry has implemented the technology in some of its wholesale banking sites thereby securing millions of dollars of transactions every day. Finally, this paper justifies the security of PKM and its flexible revocation models; and illustrates the justification with proofs through formal logic.


## 1. Introduction

Imagine a vision for Internet security where users reference a single asymmetric key pair to routinely login to multiple web sites and digitally sign transactions. Imagine if the security technology were strong enough to be permissible by banks, insurance companies, health care, government agencies, and most other business domains. Perhaps, some may argue that PKI technology already realizes this vision today; however, theory differs from practice from the perspective of interoperability.

For example, suppose an insurance company were to issue a certificate to a user, but mistakenly identifies that user incorrectly. Further suppose that the user were a medical doctor authorized to prescribe medication; and the insurance company inadvertently issues the certificate to an adversary who prescribes medication for nefarious

* Corresponding author. Tel.: +1 315 395 9182.
*E-mail addresses:* glenn.benson@jpmchase.com (G. Benson), skchin@syr.edu (S.-K. Chin), sbcroston@statestreet.com (S. Croston), karjay@microsoft.com (K. Jayaraman), sbolder@syr.edu (S. Older).

[1] The author did this work during the time he worked for JP Morgan Chase & Co.

[2] The author did this work while he was graduate student at Syracuse University.

[3] The authors of this paper are solely responsible for the content thereof. The paper does not reflect the views or the official policy of JPMorgan Chase & Co.

http://dx.doi.org/10.1016/j.comnet.2014.03.024
1389-1286/

purposes resulting in injury or death. Which organization is at fault? The legitimate doctor is a victim as opposed to a perpetrator because the doctor may have been unaware of the insurance company's mistake. Because of this scenario, the insurance company normally chooses to opt-out of interoperability, thereby avoiding the possibility of many potential lawsuits. That is, the insurance company may potentially distribute certificates to its own users, but does not encourage or participate in certificate sharing across web sites not owned by the bank. Unfortunately, by choosing to opt-out, the Internet cannot realize its interoperability vision. The result is the situation in which we find ourselves today where the Internet exhibits insufficient security; and the users complain about a proliferation of passwords that they cannot handle.

Alternatively, one may potentially consider Single Sign-on technology as a solution for interoperability. However, while Single Sign-on effectively provides federated identity, Single Sign-on fails to meet the digital signature requirement. Consider the situation in which a bank executes a payment moving millions of dollars to a beneficiary. Subsequently, the user denies the payment and requests a refund. In order to help adjudicate the dispute, a digital signature's non-repudiation capability may prove beneficial. By analyzing the signature, a judge can determine whether the transaction's signer had possession of the required asymmetric private key; and the judge can identify whether the transaction amount or beneficiary may have been tampered.

By providing key management technology that interoperates between any web site, even those that handle million dollar payments, everyone benefits by amortizing the cost of security over multiple sites. Suppose each user were to obtain a physical security credential that locks an asymmetric private key. While the private key cannot leak off the credential, the credential has the computing capability to perform asymmetric cryptographic operations. In the absence of interoperability, security credentials have limited practicality because a user requires a separate credential for each web site. However, if all of the user's web sites offered interoperable security, then the user would only need a single credential to login and sign transactions everywhere. If a user could use the same credential for many different sites, then the user may be more willing to procure improved security credential hardware. For example, one user may choose to lock his or her key pair in an encrypted file on a smart phone. Another user may lock the key pair on a secured, cryptographically enhanced USB token. A third user may lock the key pair on a cryptographically enhanced token that only unlocks after providing a thumbprint. Credential vendors could continually improve by offering technology at different price points and levels of security. Ultimately, everyone wins: the Internet becomes simpler because each user gets a single credential; the Internet web sites raise their security because digital signature technology becomes commonplace; and credential technology upgrades because users voluntarily choose to upgrade to better technology.

This paper provides a key management solution that realizes the interoperable Internet security vision by directly addressing the liability concern without sacrificing security or interoperability. For clarity, this paper makes three simplifying assumptions. First, the paper bypasses the potential privacy problem by assuming that each user has a single key pair. In practice, a user may potentially wish to create multiple virtual identities each represented by a key pair, but this paper simplifies by assuming only one identity per user. Second, this paper describes digital signatures, but does not detail login events. In practice, a login event is a simple extension of a digital signature that requires a user to sign a random number chosen by the web site. Third, this paper narrows the domain to wholesale banking by describing a technology that allows a user to employ a single key pair to sign transactions at multiple banks. Wholesale banking is a microcosm of the greater Internet security problem because it focuses upon the liability concern. If Bank-A and Bank-B were to each allow a user to authorize a multi-hundred million dollar payment with the same certificate, then one may intuitively extend the security technology beyond banking to other areas such as healthcare, tax payments, or other domains.

The technology described in this paper is not merely a proposal. Rather, the financial services industry has implemented the technology thereby securing millions of dollars of transactions every day. We call this technology Partner Key Management (PKM). Since wholesale banking permits transactions of ultra-high value, we believe that a demonstration within the wholesale banking domain validates an extension to many other business domain. The prevailing security solution is traditional Public Key Infrastructure (PKI) [1], but PKI is an ill-fit for interoperable wholesale banking due to insufficiencies in the liability model. The first insufficiency relates the Certificate Authority (CA) – a benevolent party which is a fundamental building block of a PKI. In a high-risk environment, practically no CA has the financial resources required to accept a liability burden associated with multi-million dollar payments. For example, suppose a CA issues a certificate; and a multi-million dollar fraudulent transaction were executed with that certificate. If fault were somehow conferred upon the CA, then few (if any) CAs in the industry today would be willing or able to make their customers whole by reimbursing the lost funds. This paper explains that in a PKI, one needs to trust both the CA and the parties in the corporation authorized to direct the CA to execute actions such as create or revoke certificates. In contrast, in PKM, we need to trust the same parties in the corporation, but we can simply eliminate the CA. PKM shifts trust toward bilateral agreements.

In addition, when one further considers interoperability in a high-risk environment, then PKI's Registration Authority (RA) also tends to fail its liability requirements. In an interoperable environment, all participating parties should accept digital signatures executed using certificates authorized by all RAs. Suppose a fraudulent hundred-million dollar transaction were identified; and an RA were found to have issued a certificate to an adversarial party. Since no RA wishes to subscribe to an unlimited liability model, no RA agrees to make all harmed parties whole.

J.P. Morgan operates a PKM service which directly connects customer payment engines to the bank servers via a file-based communication channel. Customers may