Credentials Management for High-Value Transactions

Glenn Benson[1] Shiu-Kai Chin[2] Sean Croston[1]
Karthick Jayaraman[2] Susan Older[2]

[1]Treasury Services,
JPMorgan Chase, Inc

[2]Dept. of EECS,
Syracuse University

Mathematical Methods, Models, and Architectures for Computer Network Security (MMM ACNS) 2010

High Value Online Transactions

- Wholesale banking
  - Customers : large corporations and governments
  - Transaction statistics
    - $58 millions per second
    - $5.1 Trilion - one-day maximum
- Security requirement
  - Assurance of trustworthiness
- Business requirement
  - Interoperable credentials

Public Key Infrastructure

PKI Providers

- A third party who provides credentials to a subscriber, corporations in our case
- Provides validation services to the relying party, Banks in our case

Banks - *Relying Party*

- Receive a transaction signed with a credential
- Connect to the appropriate PKI provider using their protocol to validate the credential

Corporations - *Subscribers*

- Obtains a credential from a PKI provider
- Wants the credential to be accepted by all banks

PKI is a poor match for wholesale banking

Liability

- A PKI provider vouches for the crdential, but will not accept liability
- Authorization is outside the scope of their services

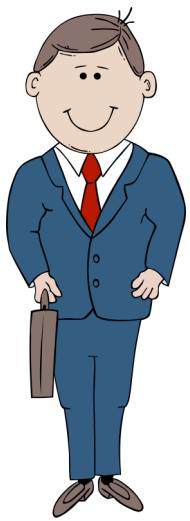
Multiple Validation Protocols

- Banks have to deal with the protocols of each PKI provider
- Maintaining infrastructure for dealing each PKI provider is costly

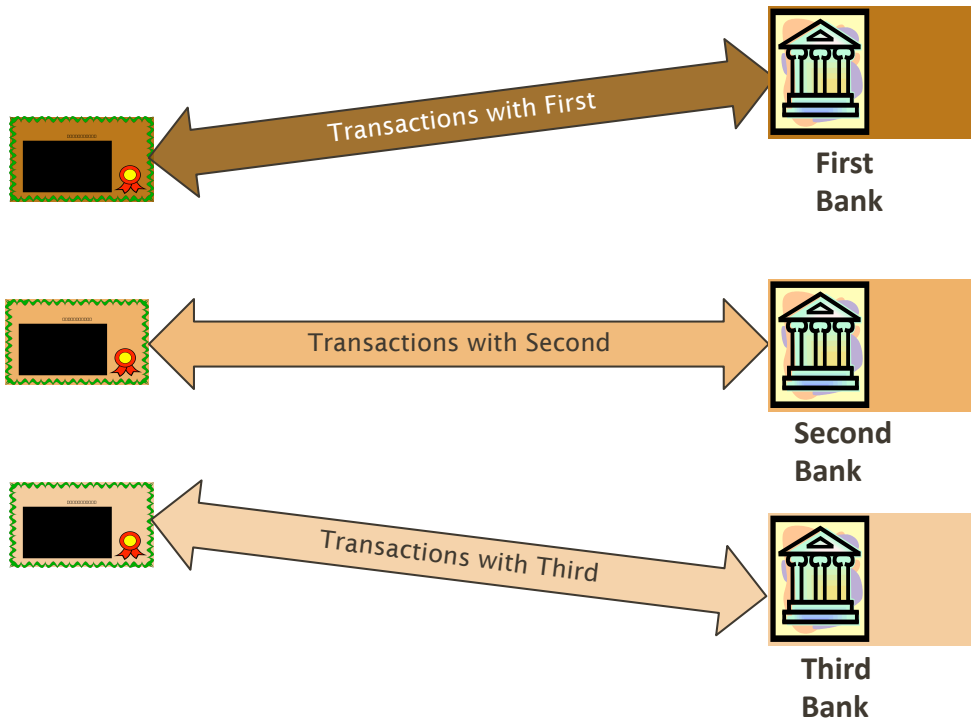
One size does not fit all

- PKI assumes uniform controls
- Banks need to enforce controls depending on bilateral agreements

Each Bank Trusts Itself Only



Bob
Cash Manager
Widget



Purpose and Preview

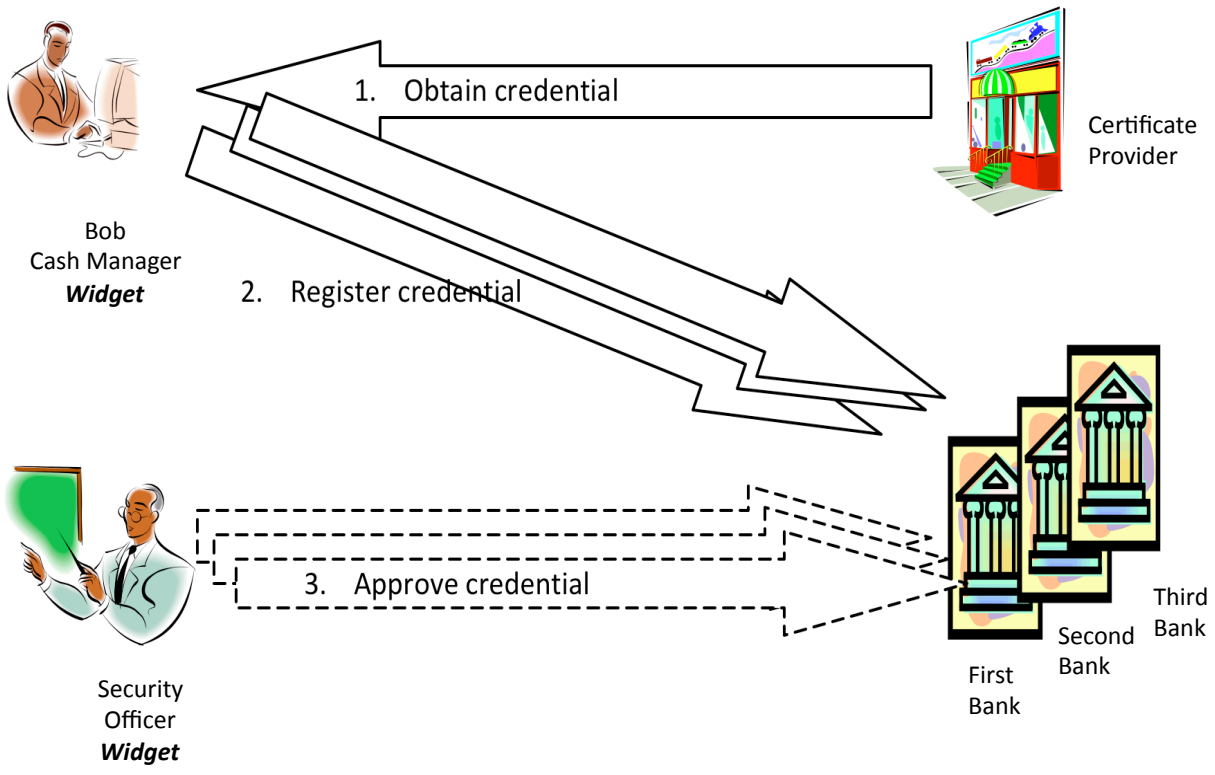
Purpose

- Introduce Partner Key Management (PKM)
- Describe our assurance approach

Preview

- Overview of PKM
  - Interoperable credentials
  - Varying controls
  - Flexible trust models
- Formal Analysis

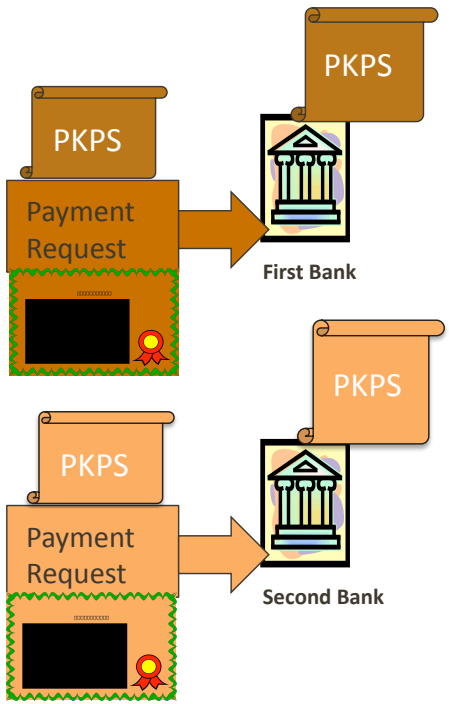
Credential Registration



Credential Registration

Varying Controls

- Controls and limits on credentials
  - Agreed bilaterally between partners
  - Varies between partners
- Partner Key Practice Statement (PKPS)
  - Machine readable document
  - A Bank's policy on credentials
  - Specific to a partner and a set of transactions



Partner Key Practise Statement

- Specifies four types of controls
  - Credential policy
  - Revocation policy
  - Timestamp policy
  - Signature policy
- A type of WS-Policy

Flexible Trust Models

Sender Validation with Evidence

- Signer connects to the PKI provider and validates the key
- Signs the validation certificate and includes it in the transaction

Sender Validation without Evidence

- Corporation has a proprietary protocol for communicating the key status to the bank
- Bank validates the key based on the key status

Receiver Validation

- Bank connects to PKI provider to validate the keys

Assurance Approach

- Access-control logic
  - Modification of multi-agent propositional modal logic created by Abadi, Burrows, Lampson, and Plotkin
  - Implemented as a conservative extension to the Cambridge Higher Order Logic (HOL-4) Kananaskis 5 theorem prover
- Used to
  - Describe the protocol
  - Assure the logical consistency of operations
  - Make trust assumptions explicit

Inference Rules

Rules

- Inconvenient to use Kripke semantics
- Use inference rules $\dfrac{H_1 \cdots H_n}{C}$ instead

Soundness

$\dfrac{H_1 \cdots H_n}{C}$ is sound if *for all Kripke structures* $\mathcal{M}$ and each $i \in \{1, \ldots, n\}$:

$$\text{If } \mathcal{E}_{\mathcal{M}}[\![H_i]\!] = W \text{ then } \mathcal{E}_{\mathcal{M}}[\![C]\!] = W$$

- All rules are sound
- All verified in HOL-4 K-5 theorem prover

Core inference rules

Taut $\dfrac{}{\varphi}$ if φ is an instance of a prop-logic tautology

Modus Ponens $\dfrac{\varphi \quad \varphi \supset \varphi'}{\varphi'}$ *Says* $\dfrac{\varphi}{P \text{ says } \varphi}$

MP Says $\dfrac{}{(P \text{ says } (\varphi \supset \varphi')) \supset (P \text{ says } \varphi \supset P \text{ says } \varphi')}$

Speaks For $\dfrac{}{P \Rightarrow Q \supset (P \text{ says } \varphi \supset Q \text{ says } \varphi)}$

Quoting $\dfrac{}{P \mid Q \text{ says } \varphi \equiv P \text{ says } Q \text{ says } \varphi}$

&Says $\dfrac{}{P\&Q \text{ says } \varphi \equiv P \text{ says } \varphi \wedge Q \text{ says } \varphi}$ *Idempotency of* $\Rightarrow$ $\dfrac{}{P \Rightarrow P}$

Monotonicity of $\mid$ $\dfrac{P' \Rightarrow P \quad Q' \Rightarrow Q}{P' \mid Q' \Rightarrow P \mid Q}$ *Associativity of* $\mid$ $\dfrac{P \mid (Q \mid R) \text{ says } \varphi}{(P \mid Q) \mid R \text{ says } \varphi}$

P controls $\varphi \stackrel{\text{def}}{=} (P \text{ says } \varphi) \supset \varphi$ P reps Q on $\varphi \stackrel{\text{def}}{=} P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi$

First Bank

Uses PKM and Sender Validation without Evidence

Request

1. K_{Alice} says $\langle transfer\ \$10^6, acct_1, acct_2 \rangle$,
2. K_{Alice} says Ψ_{PKPS}

Operating Rules

1. *First* controls $(K_{Alice} \Rightarrow Alice)$,
2. K_{Alice} says $\Psi_{PKPS} \wedge \langle K_{Alice}, Active \rangle \supset First$ says $K_{Alice} \Rightarrow Alice$

Inference Rule

$$\textit{First Bank}\quad \frac{\begin{array}{c} K_{Alice} \text{ says } \langle transfer\ \$10^6, acct_1, acct_2 \rangle \\ K_{Alice} \text{ says } \Psi_{PKPS} \quad \langle K_{Alice}, Active \rangle \\ First \text{ controls } K_{Alice} \Rightarrow Alice \\ Alice \text{ controls } \langle transfer\ \$10^6, acct_1, acct_2 \rangle \\ K_{Alice} \text{ says } \Psi_{PKPS} \wedge \langle K_{Alice}, Active \rangle \supset First \text{ says } K_{Alice} \Rightarrow Alice \end{array}}{\langle transfer\ \$10^6, acct_1, acct_2 \rangle}$$

PKI vs PKM

	Public Key Infrastructure	Partner Key Management
Authority	*CA* controls $K_P \Rightarrow P$	*Bank* controls $K_P \Rightarrow P$
Certificate	*CA* says $K_P \Rightarrow P$	$\langle K_P, Active \rangle \supset$ *Bank* says $K_P \Rightarrow P$
Policy	Not Applicable	[conditions] $\supset \langle K_P, Active \rangle$

Results

- PKM trust assumptions commensurate with PKI
- PKM's reinterpretation of authority provides
  - Appropriate liability attribution
  - Flexible trust models
  - Controls based on bilateral agreements

Concluding Remarks

- Assurance for high value online transactions requires:
  - Precise statement of trust assumptions
  - Unambiguous interpretation of policies
- "*Access-control logic satisfies the need*"

  - Glenn Benson, *Security Architect, JPMorgan Chase.*
- Ongoing work
  - Additional trust models
  - Complete reference manual for the protocol