Blending Embedded Hardware OTP, SSO, and Out of Band Auth for Secure Cloud Access

Vikas Jain
Director, Product Management
Intel Corporation

Jesper Tohmo
CTO, Nordic Edge
(an Intel company)

Session ID: SP01-201
Session Classification: Intermediate

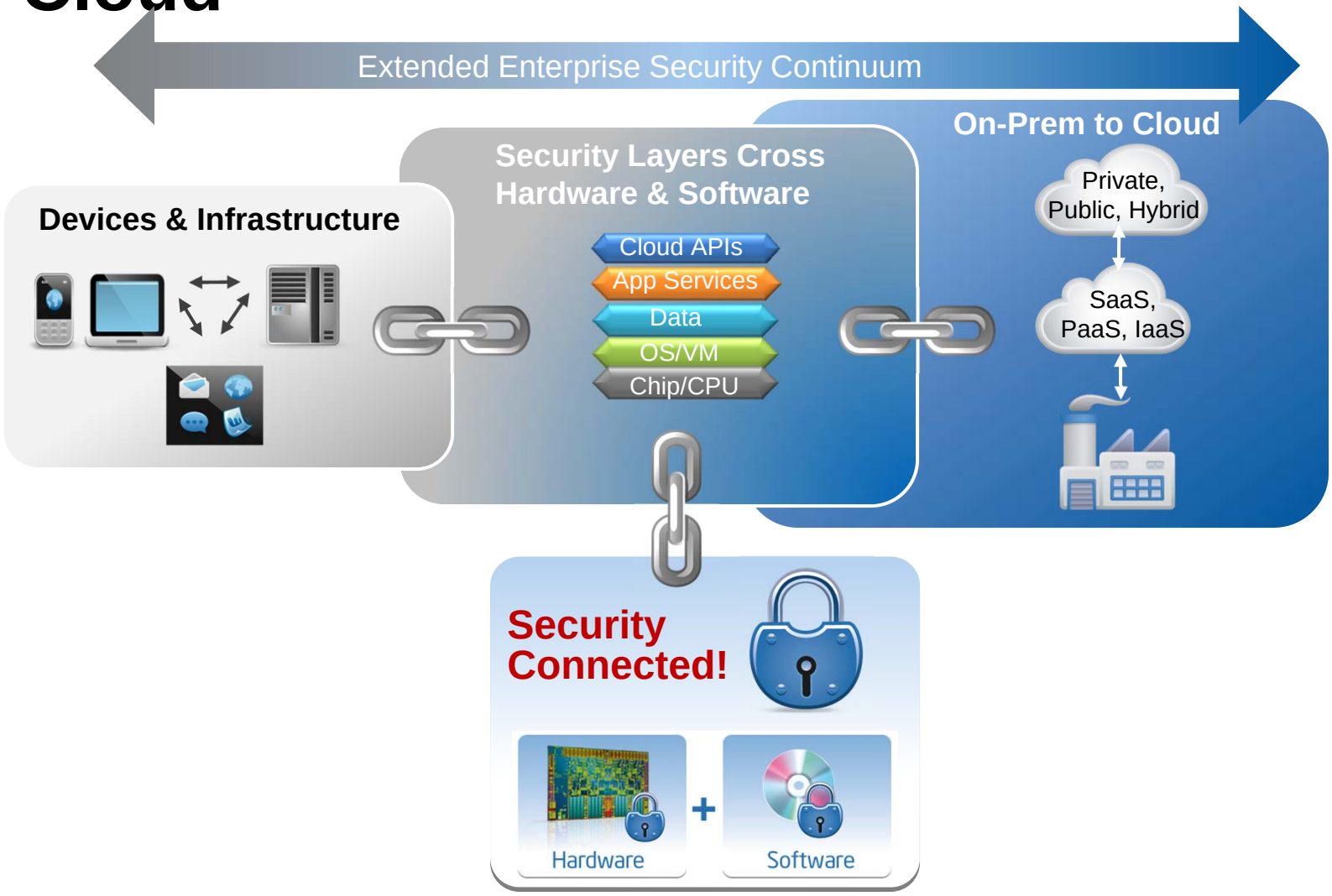
RSA CONFERENCE 2012

Agenda

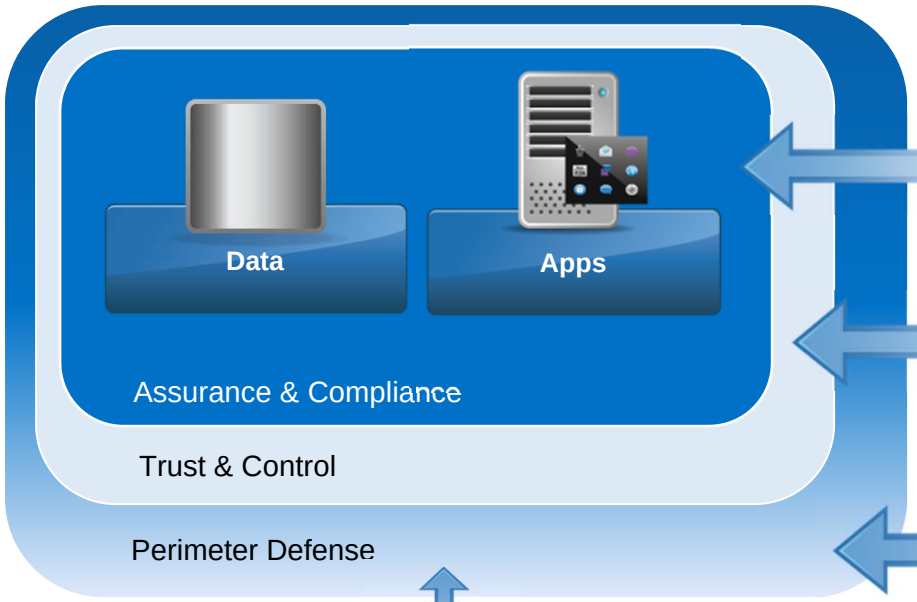
- Client to Cloud Security Layers
- User to Cloud SSO
- Strong Auth for Cloud
- Cloud App API Security
- Demo

RSACONFERENCE2012

The Goal “Security Connected” Client to Cloud



Anatomy of Client to Cloud Security Layers to Address



Assurance and Compliance: Emerging Attacks
- Data Use Policy Enforcement
- Compliance Reporting
- Pro-active SEIM integration & Alert

Trust and Control
- AuthN & AuthZ at edge tied to IdM
- Federated Trust
- Data confidentiality, PKI, Encryption

Perimeter Defense: New Attacks
- Secure Hypervisor
- Anti-Virus and Malware
- Content Threat Protection
- Secure API Management

Client Security: Traditional Attack Vector
- Protection from Malware
- Secure Federated Session
- Secure Client/Browser Exe Environment

Effective Client to Cloud Trust Involves Connecting these Layers of Cloud Security

User to Cloud Access Challenges?

Multiple Logins / Weak Security

Single Sign On (SSO) & Strong Authentication

Lack of Visibility

Centralized Management Console

Manual Provisioning

Auto Account Provisioning & Profile Sync

ID Infrastructure Integration

AuthN & Provisioning Connectors

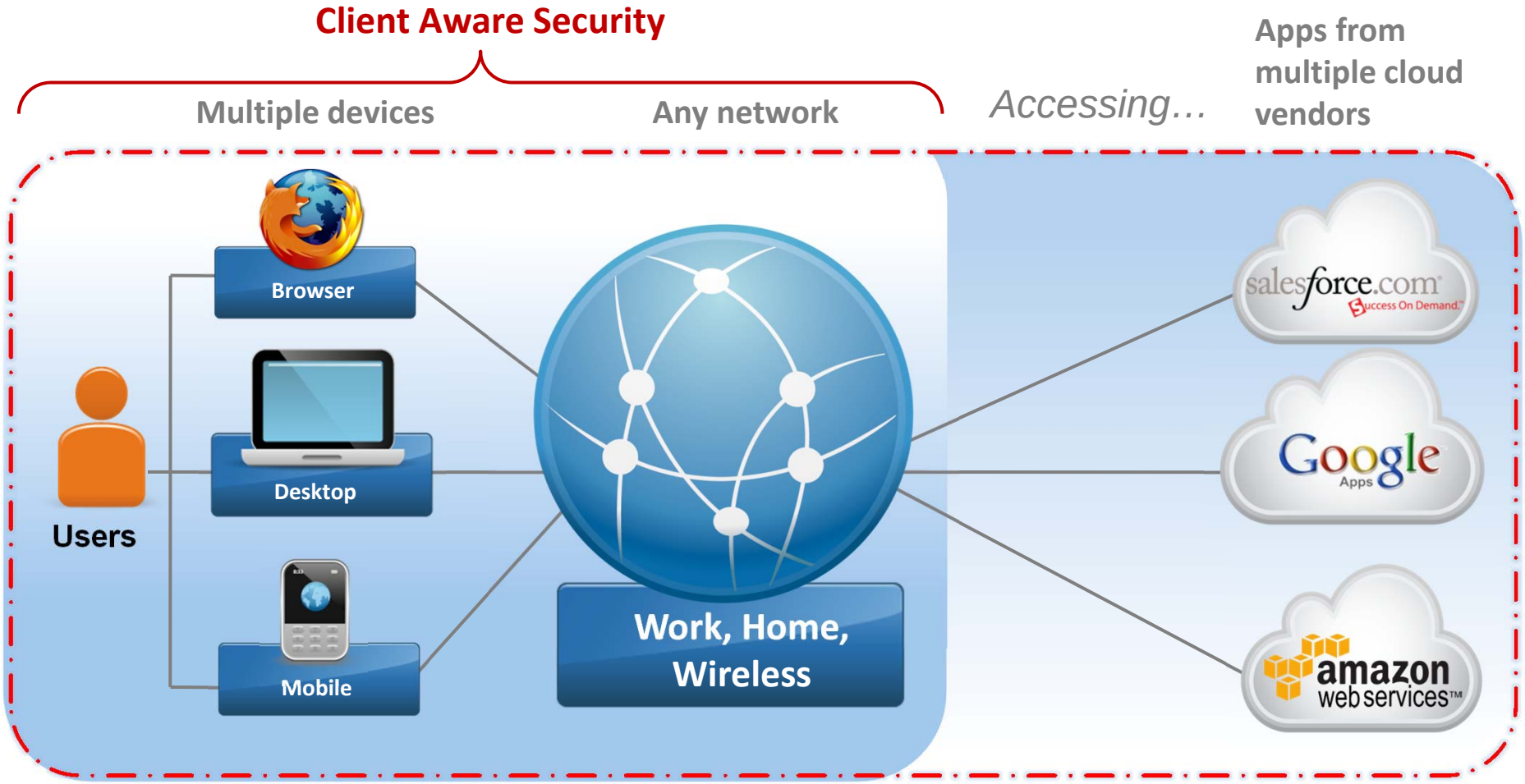
Audit Silos

Centralized Audit Logging

Scalable, Federated Trust

Standards Based

Ubiquitous Access Requirement: Any Device, Any Network, Any Cloud App



Typical solution should include …

Combine Enterprise Class Strong Auth with SSO

Provision Access

- Provision/de-provision accounts
- AD integration
- Sync Id Profiles

Adaptive Strong Auth

- Selectively apply 2nd factor OTP AuthN
- Variety of software AuthN methods & devices- mobile devices, SMS, email

Secure SSO

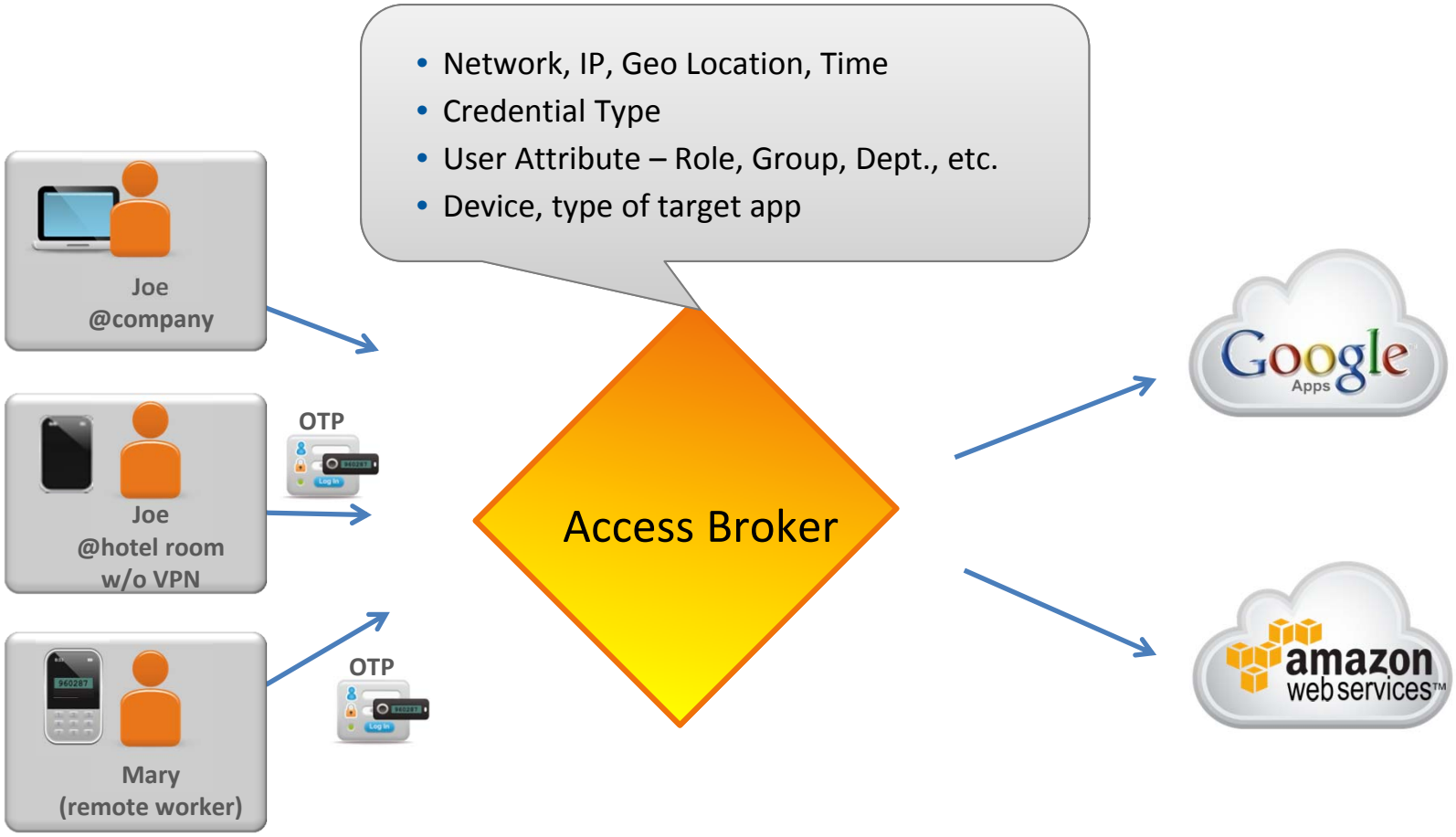
- Federate windows/AD log in via portal
- To popular SaaS like Salesforce & Google Apps

Regulatory Compliance

- Rich audit trail of user login showing AuthN level
- De-provision & orphan account reports

RSACONFERENCE2012

Client Aware, Adaptive Authentication

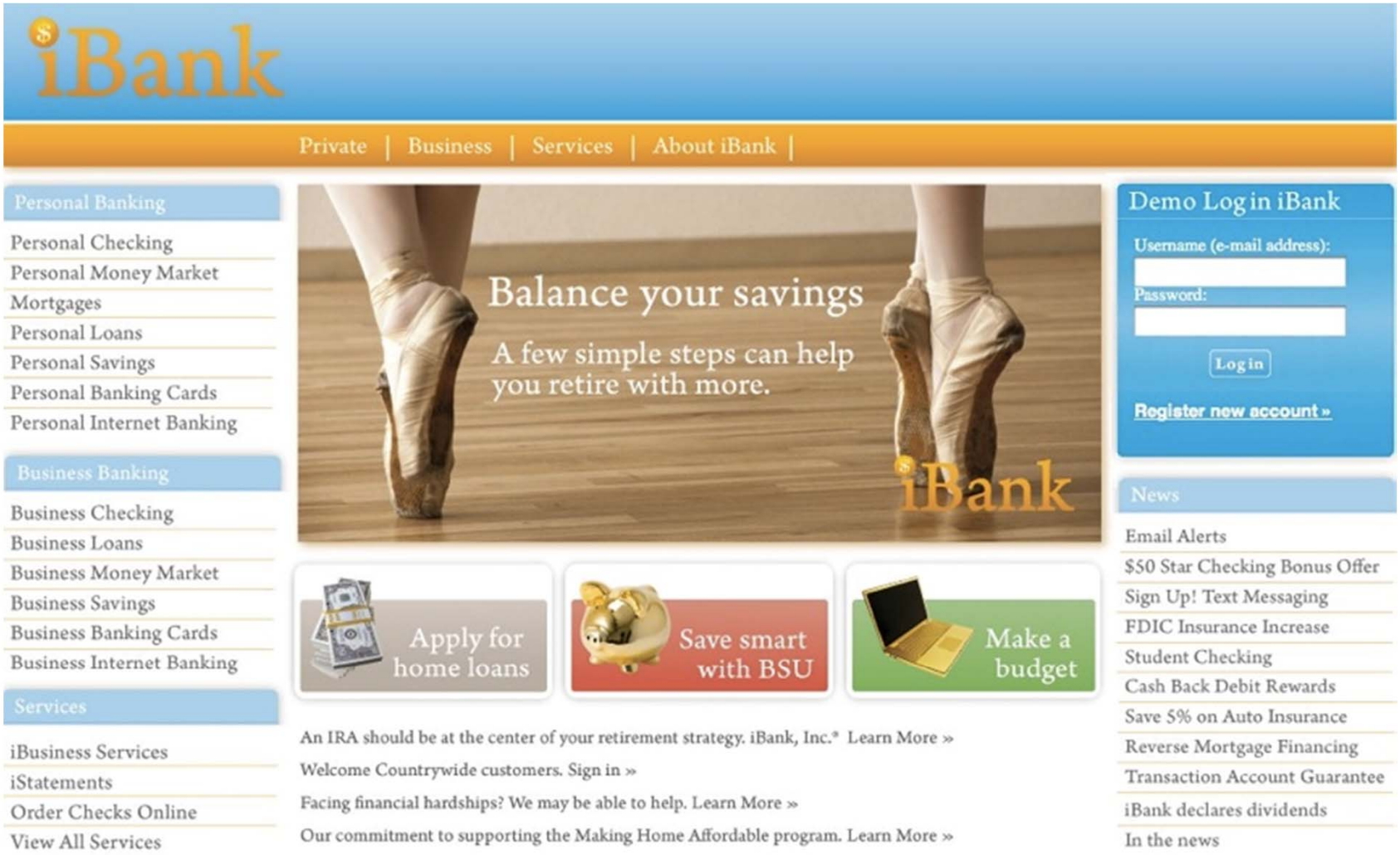


RSACONFERENCE2012

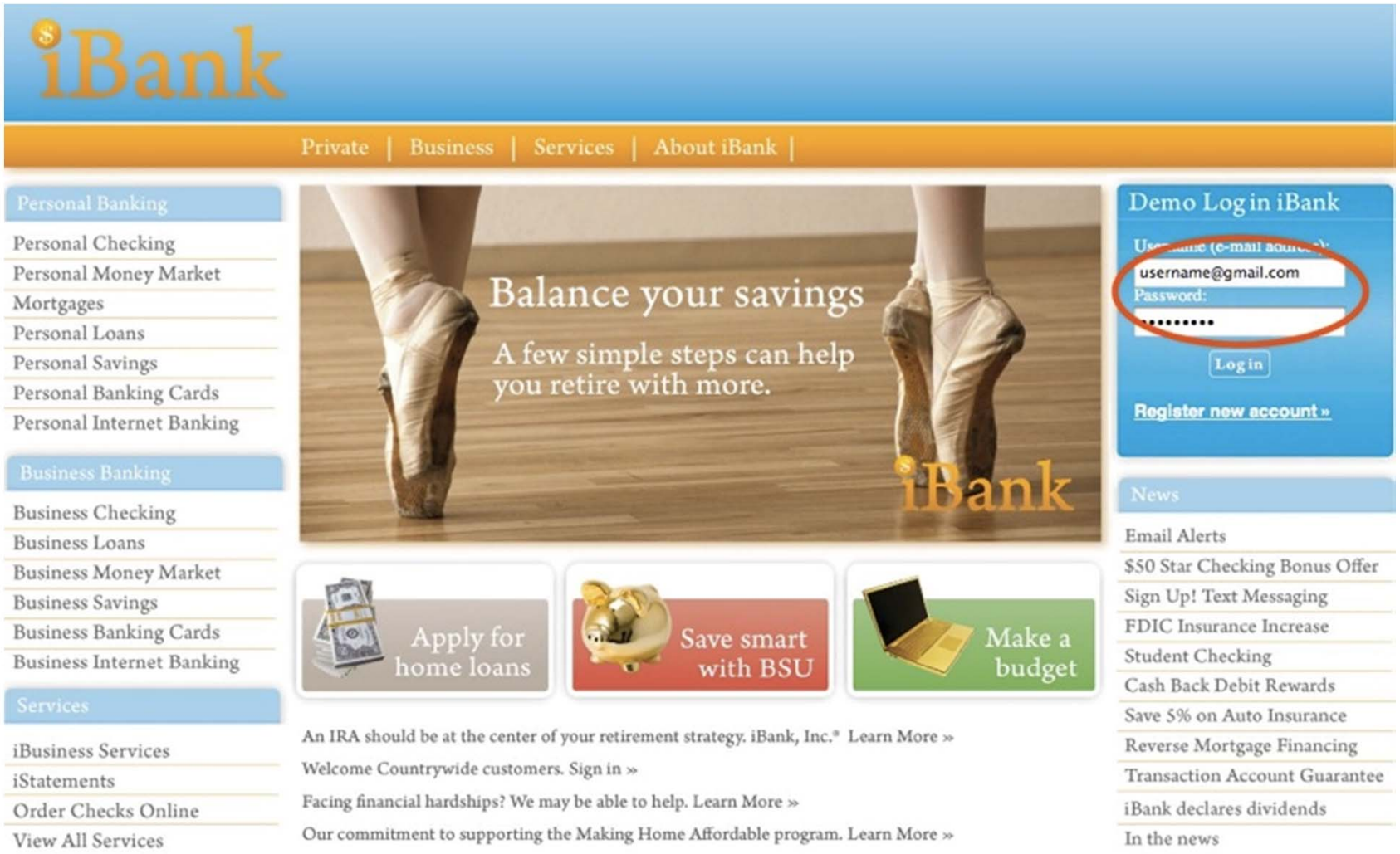
Out of band Signed Authentication

- More secure way for 2nd factor authentication
  - Authentication is performed on a separate channel different from the transaction channel
- Convenient
  - User approves using a simple Approve/Reject button from their mobile phone

Authentication

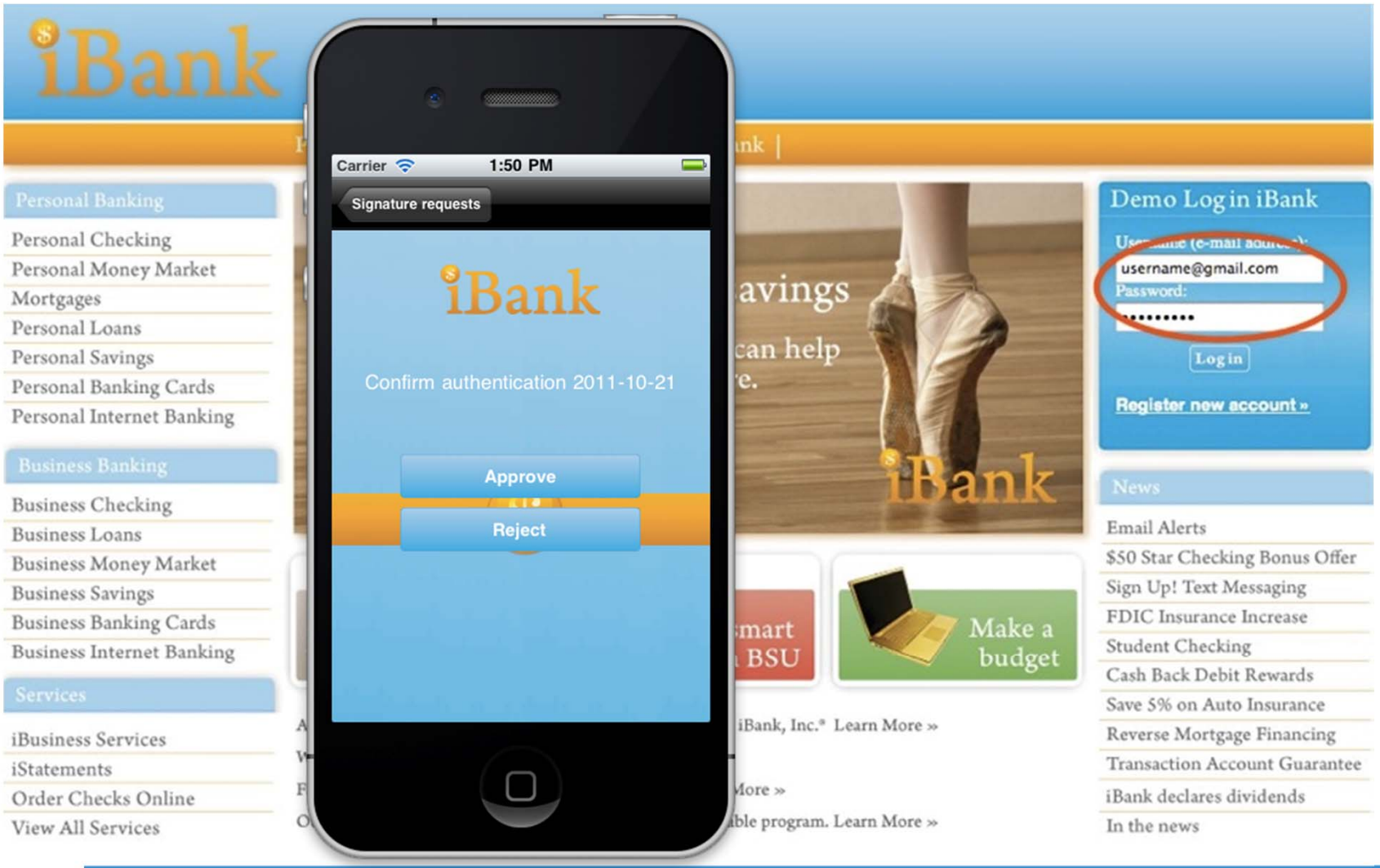


Authentication



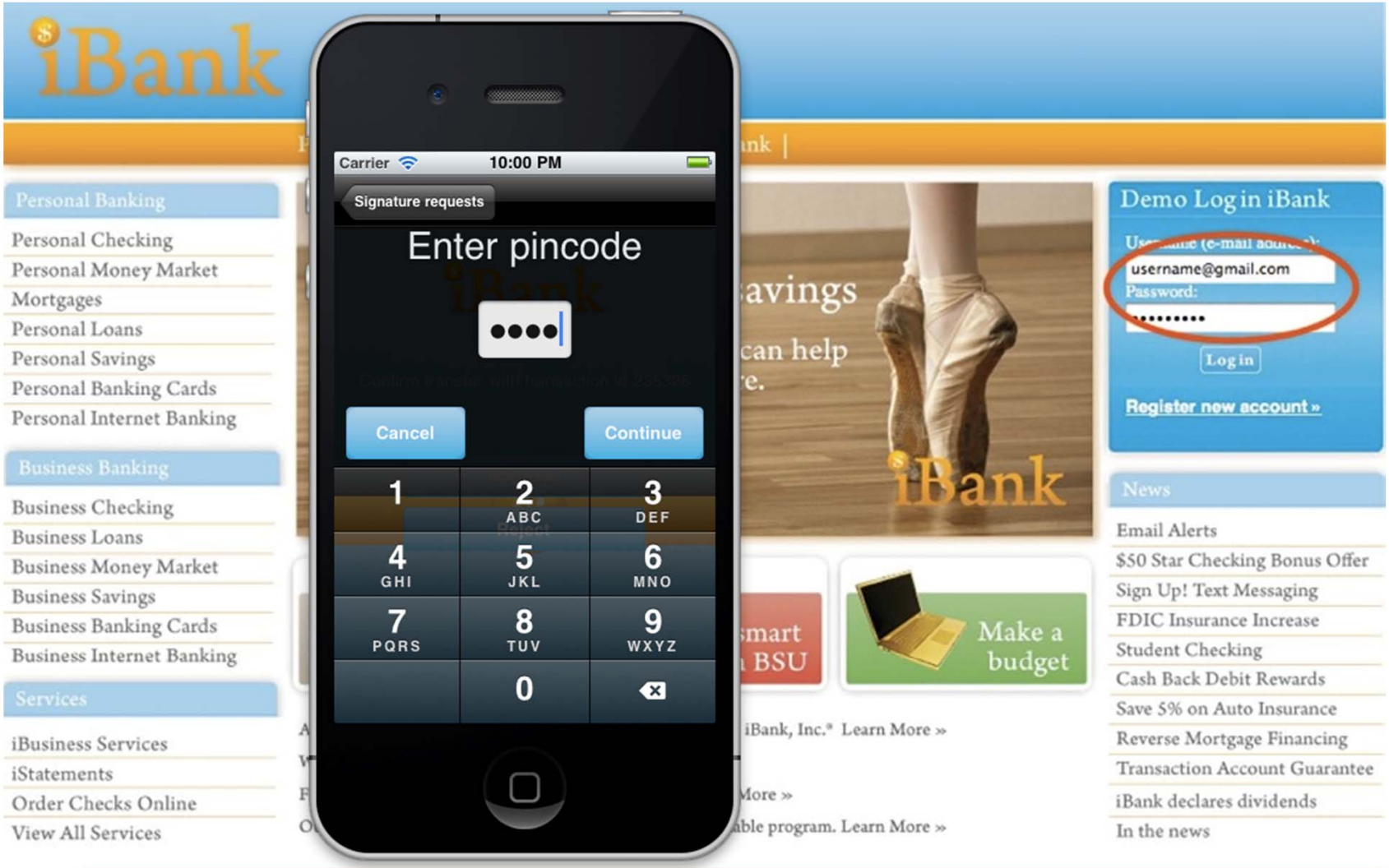
RSACONFERENCE2012

Authentication

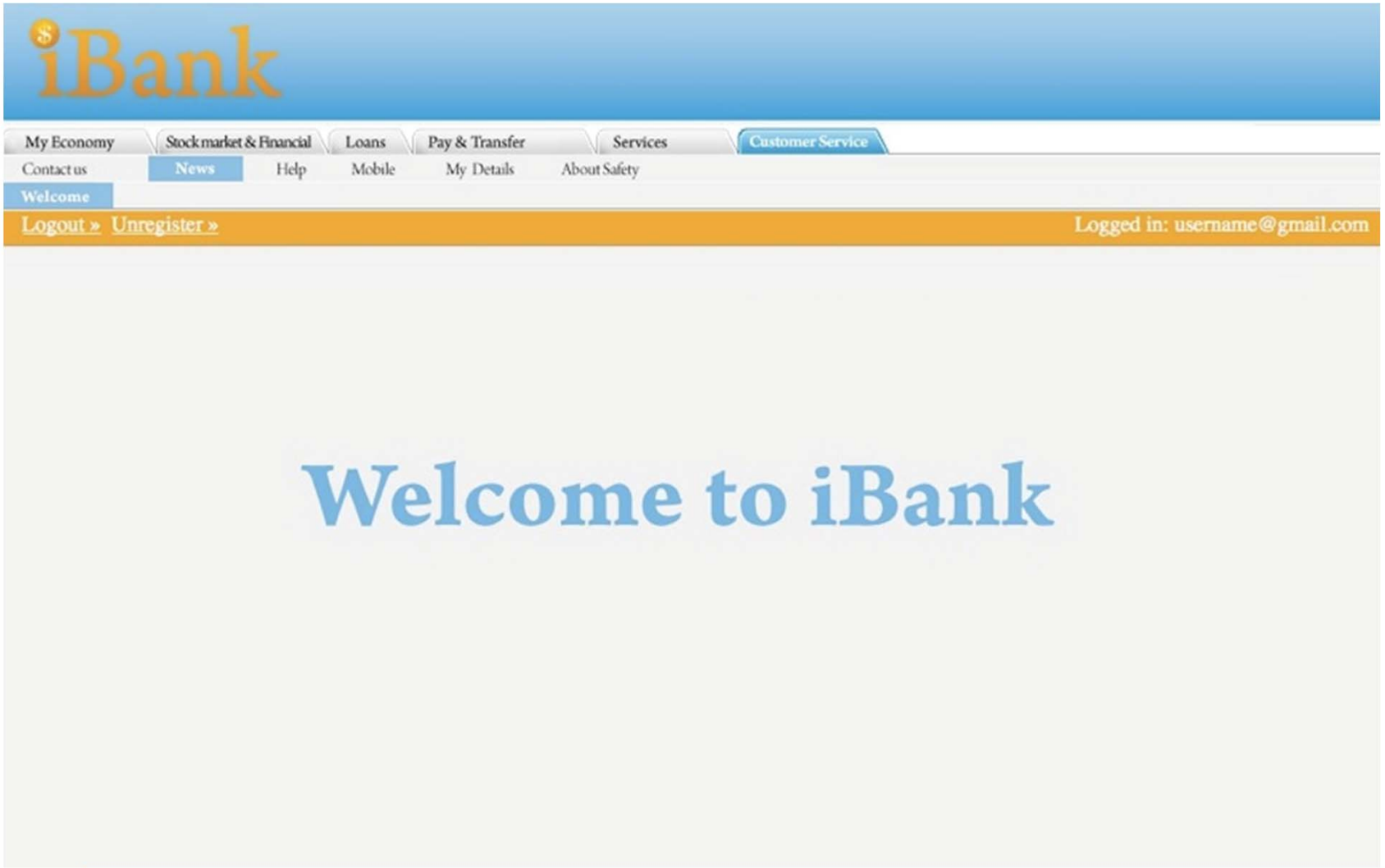


RSACONFERENCE2012

Authentication

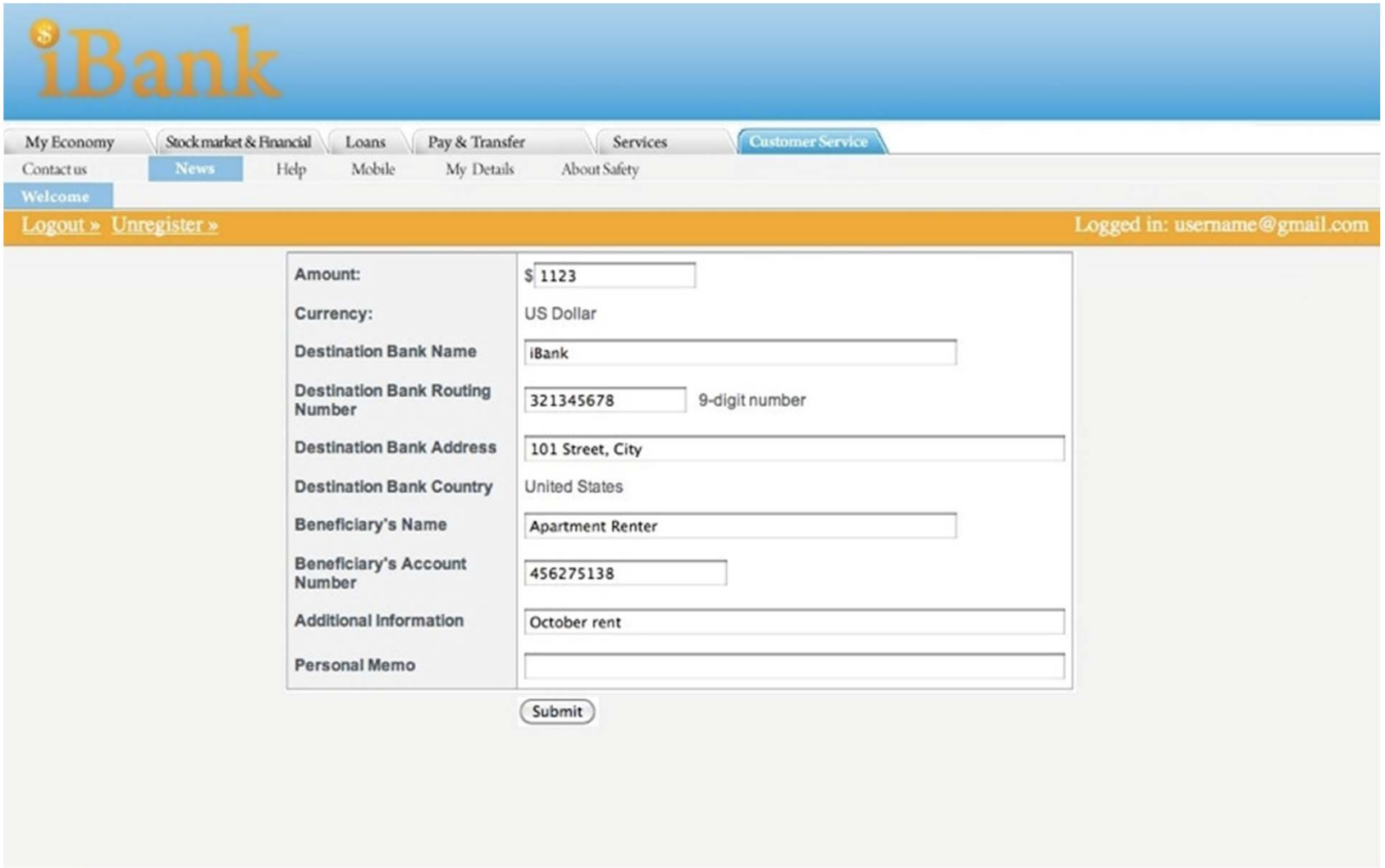


Authentication



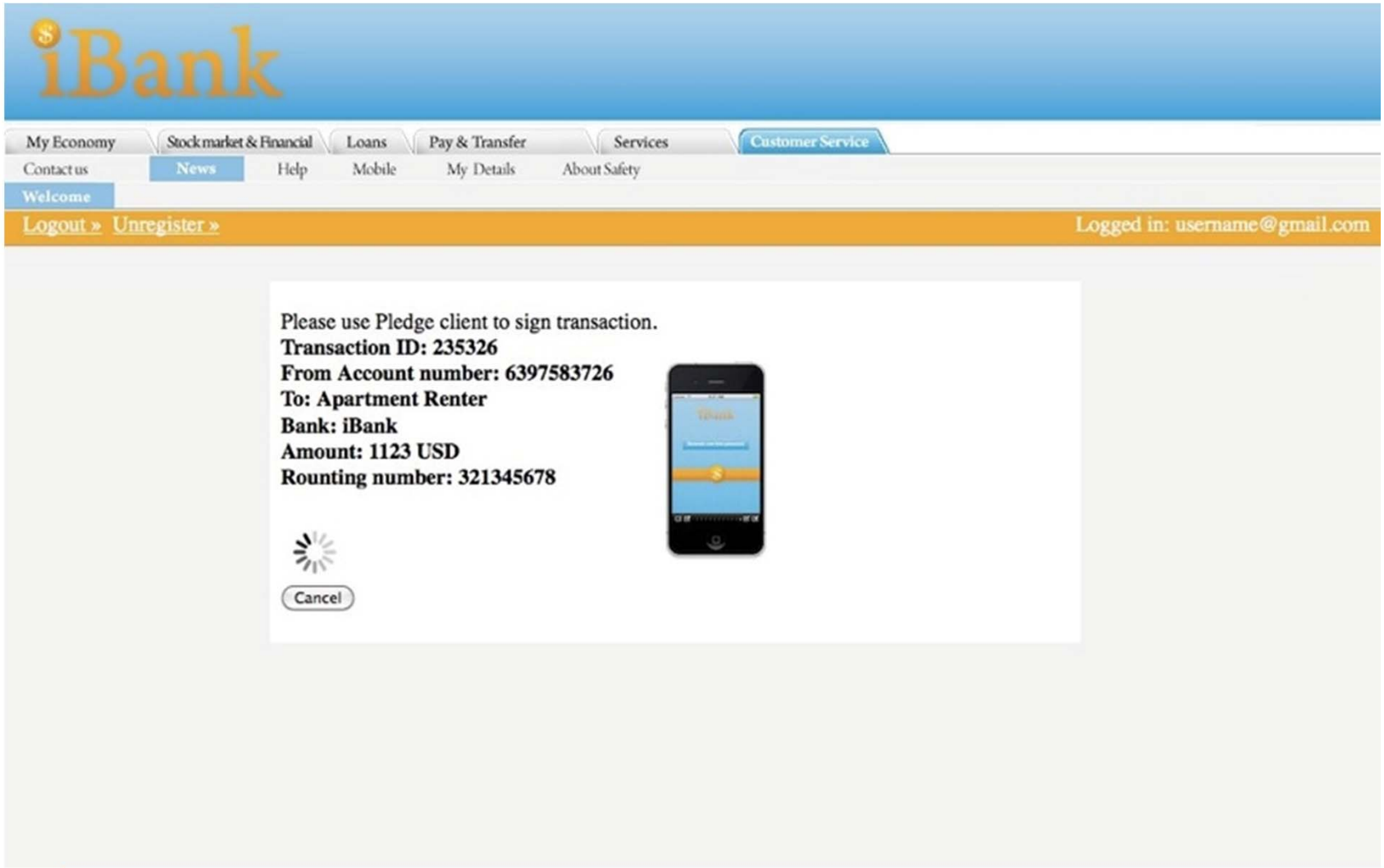
RSACONFERENCE2012

Digital Signing

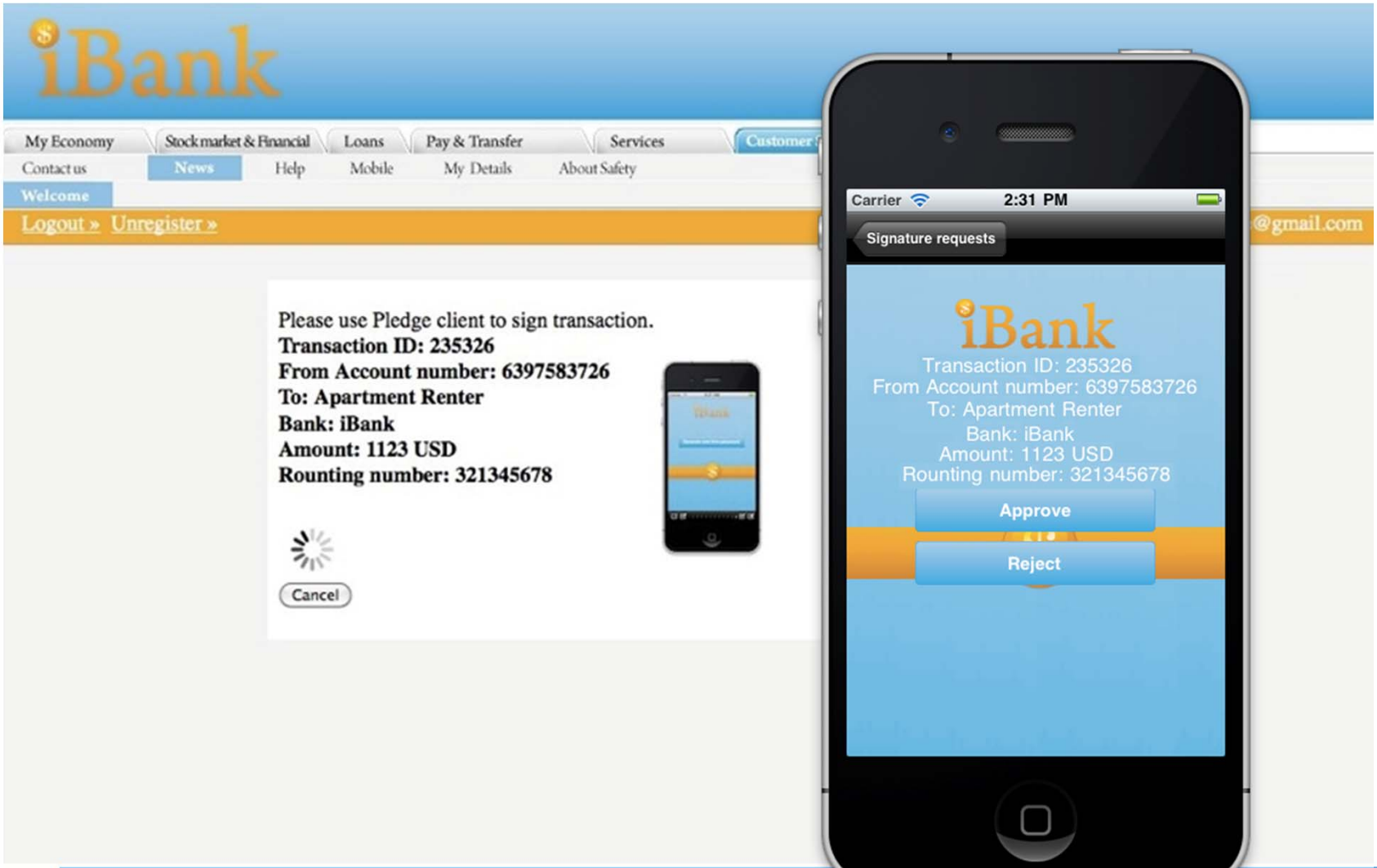


RSACONFERENCE2012

Digital Signing

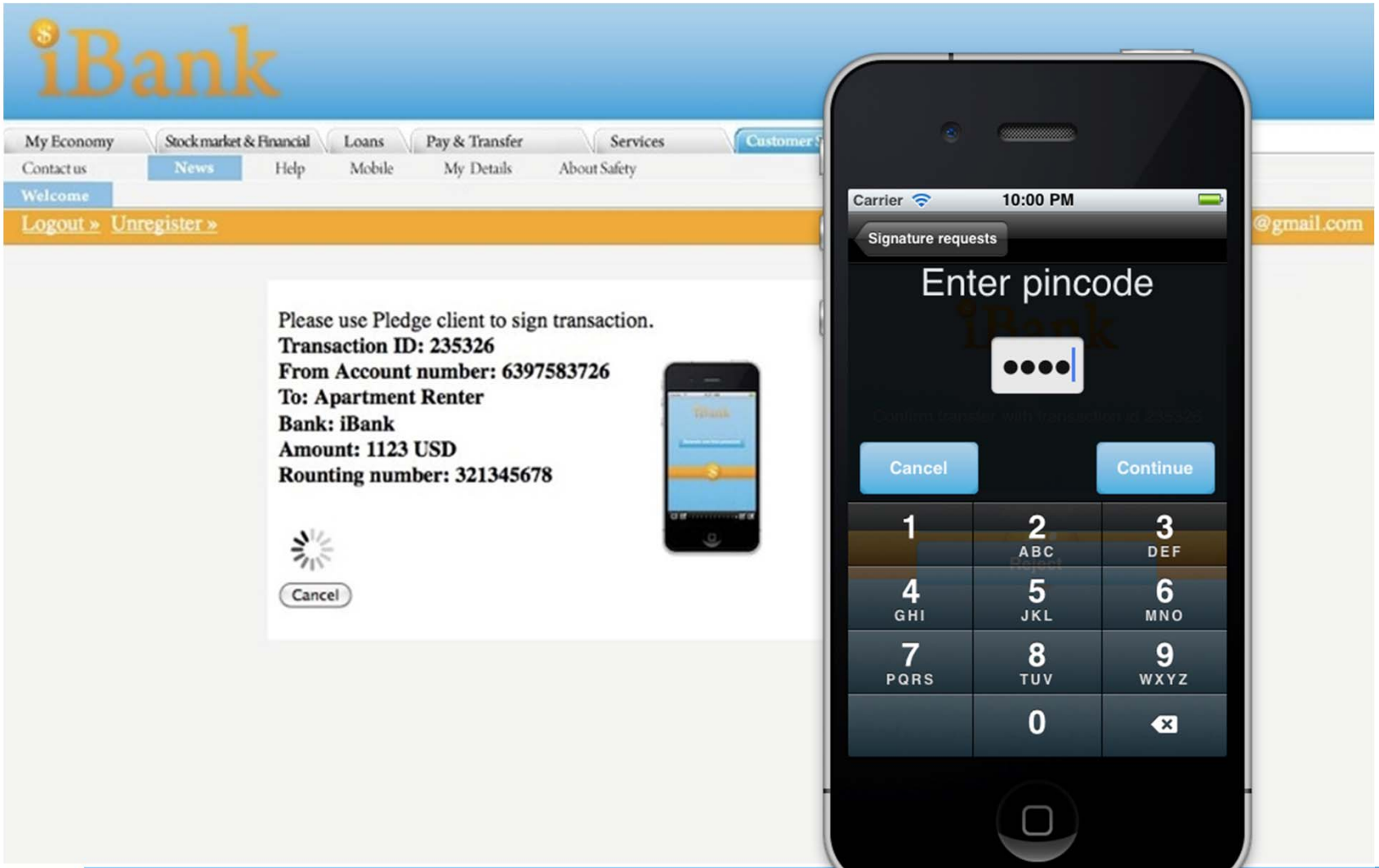


Digital Signing

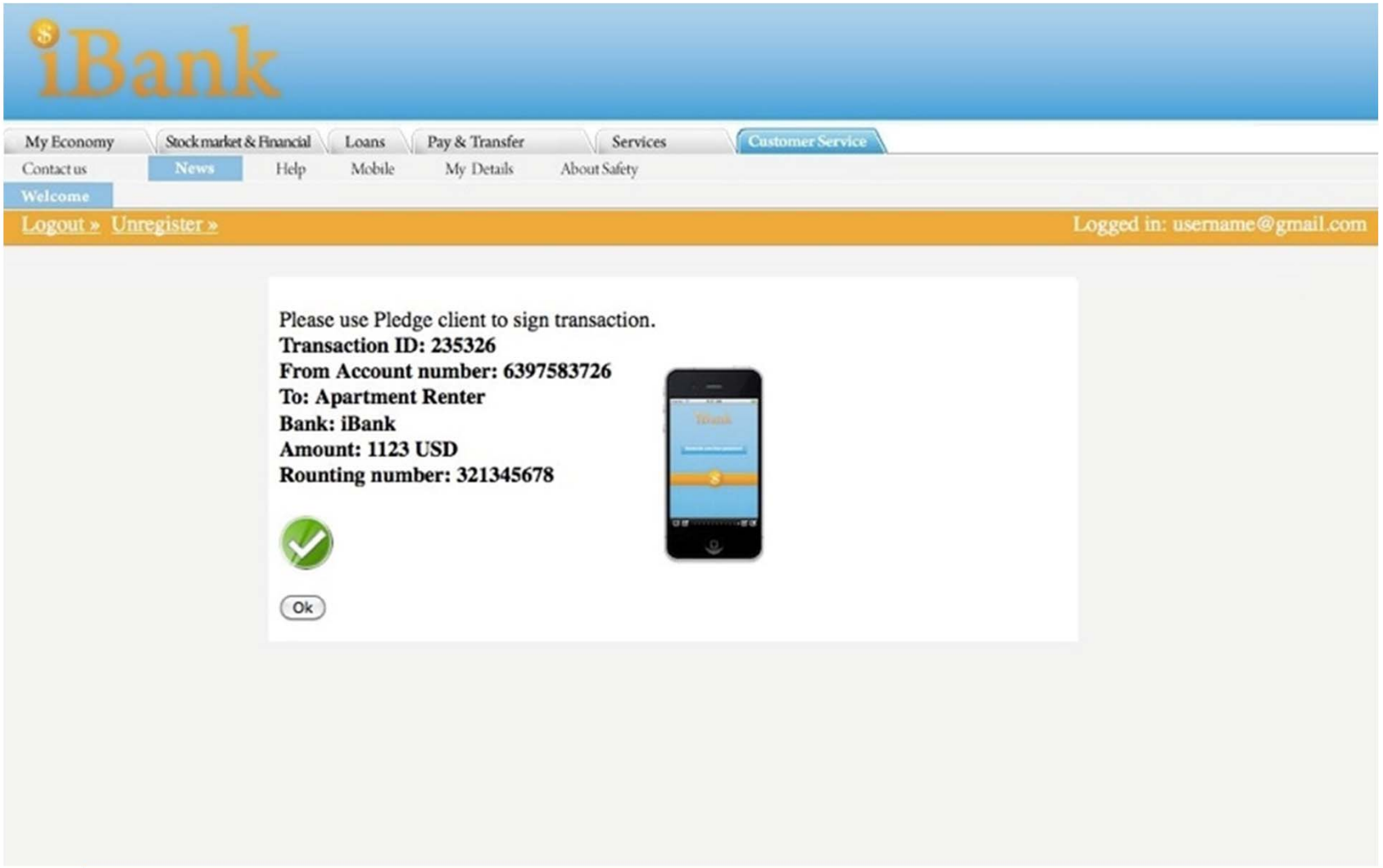


RSACONFERENCE2012

Digital Signing



Digital Signing



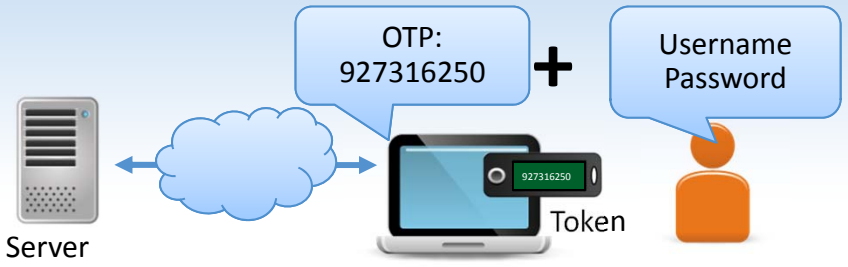
RSACONFERENCE2012

Digital Signing

RSACONFERENCE2012

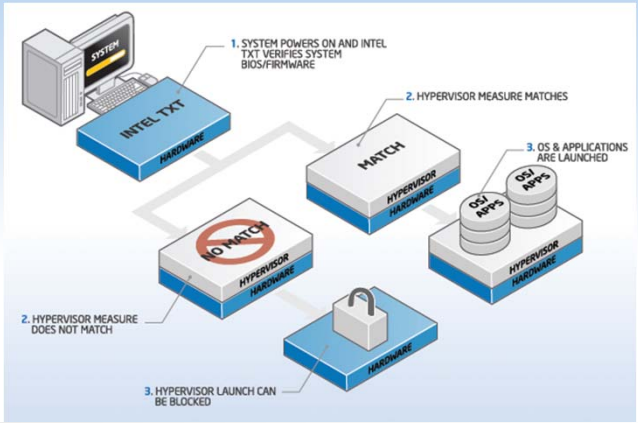
Hardware Assisted Security at the Endpoints

Silicon OTP- Enables frictionless 2-factor user authN. Determines trusted platform.



Virtual Keypad- Protects PC display from malware scraping and proves human presence at PC. Great for transaction verification and ACH fraud prevention.

TXT Data Center Root of Trust- Secure boot of VMs in Cloud



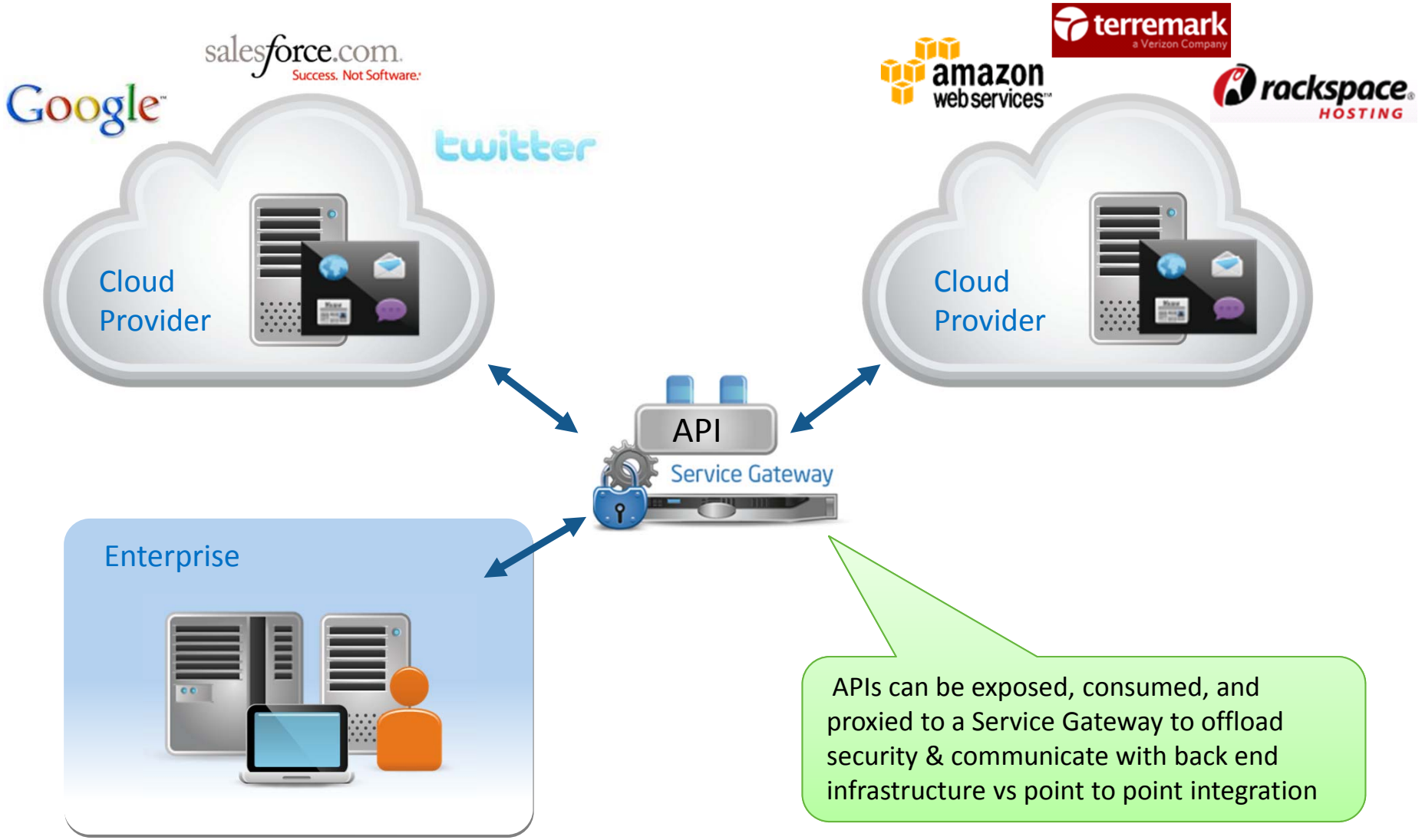
PKI certificates to authenticate User and Server to each other, digitally sign documents and emails and encrypt files and messages.

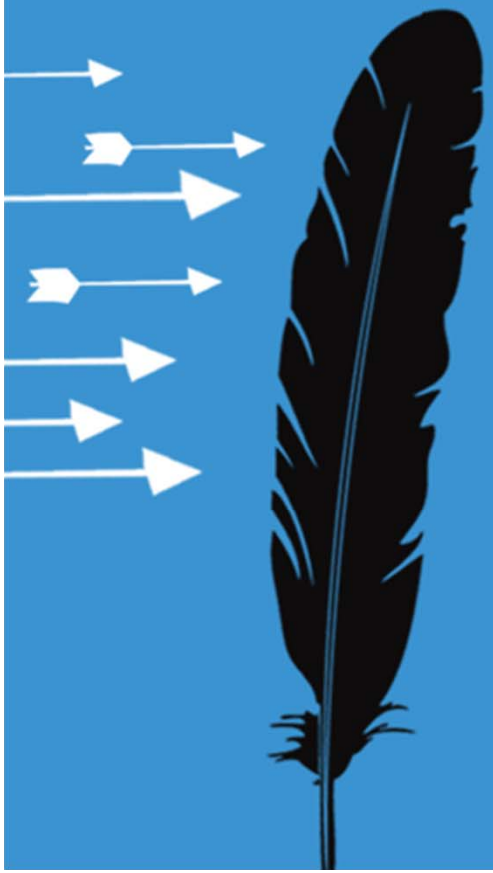
Cloud Apps- APIs are New Cloud Control Point

1/3 of Enterprise Traffic is via APIs

Google	5 billion API calls / day *(April 2010)*
facebook	5 billion API calls / day *(October 2009)*
twitter	3 billion API calls / day, 75% of all traffic *(April 2010)*
NETFLIX	20 billion API calls / month *(Jan 2011)*
ebay	8 billion API calls / month *(Q3 2009)*
bing	3 billion API calls / month *(March 2009)*
npr	1.1 billion API-delivered stories / month *(March 2010)*
salesforce.com	Over 50% of all traffic via API *(March 2008)*
amazon web services	Over 100 billion objects stored in S3 *(March 2010)*

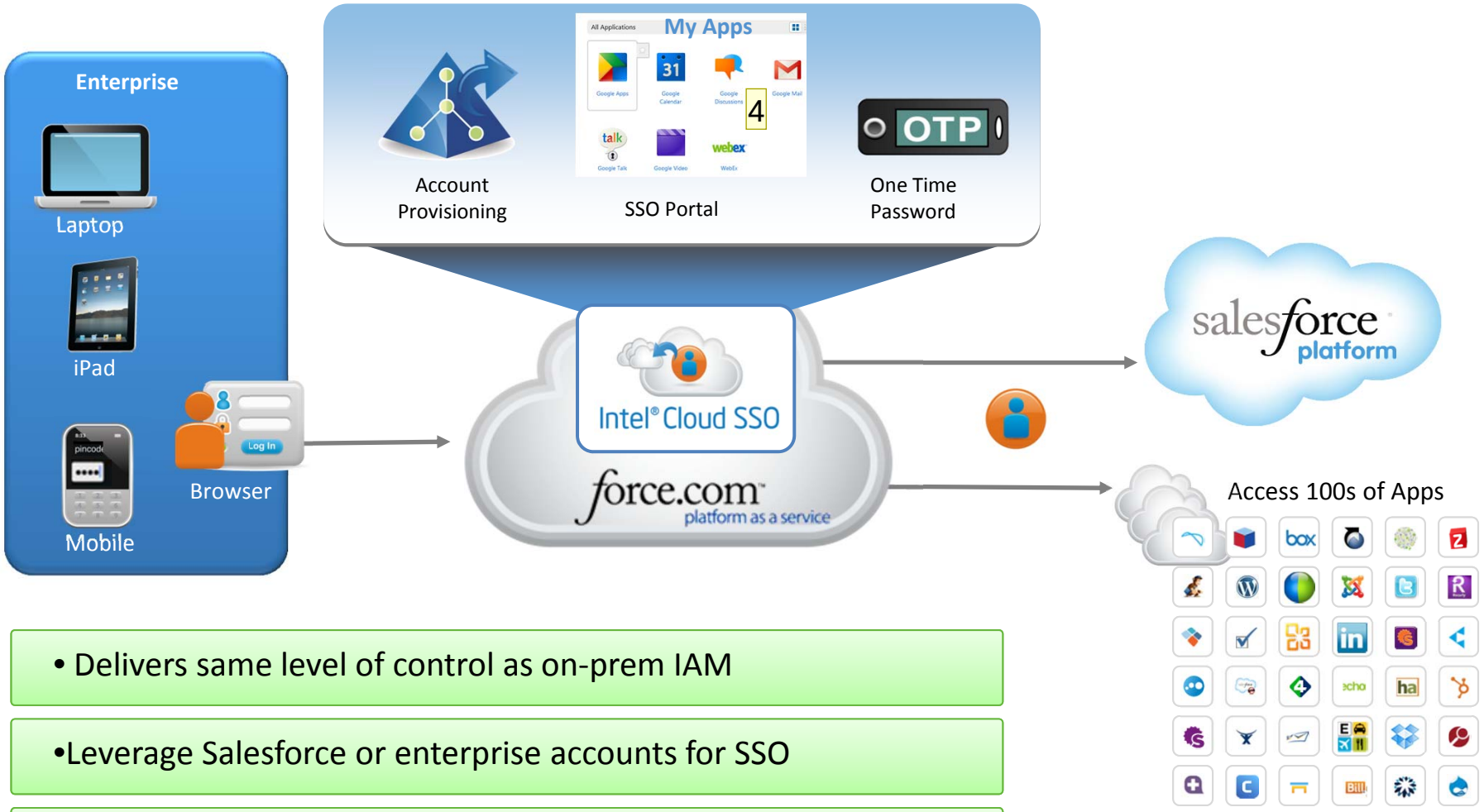
Service Gateway Broker Technology Makes a lot of Sense





Demo

Demo 1- 100% In the Cloud SSO



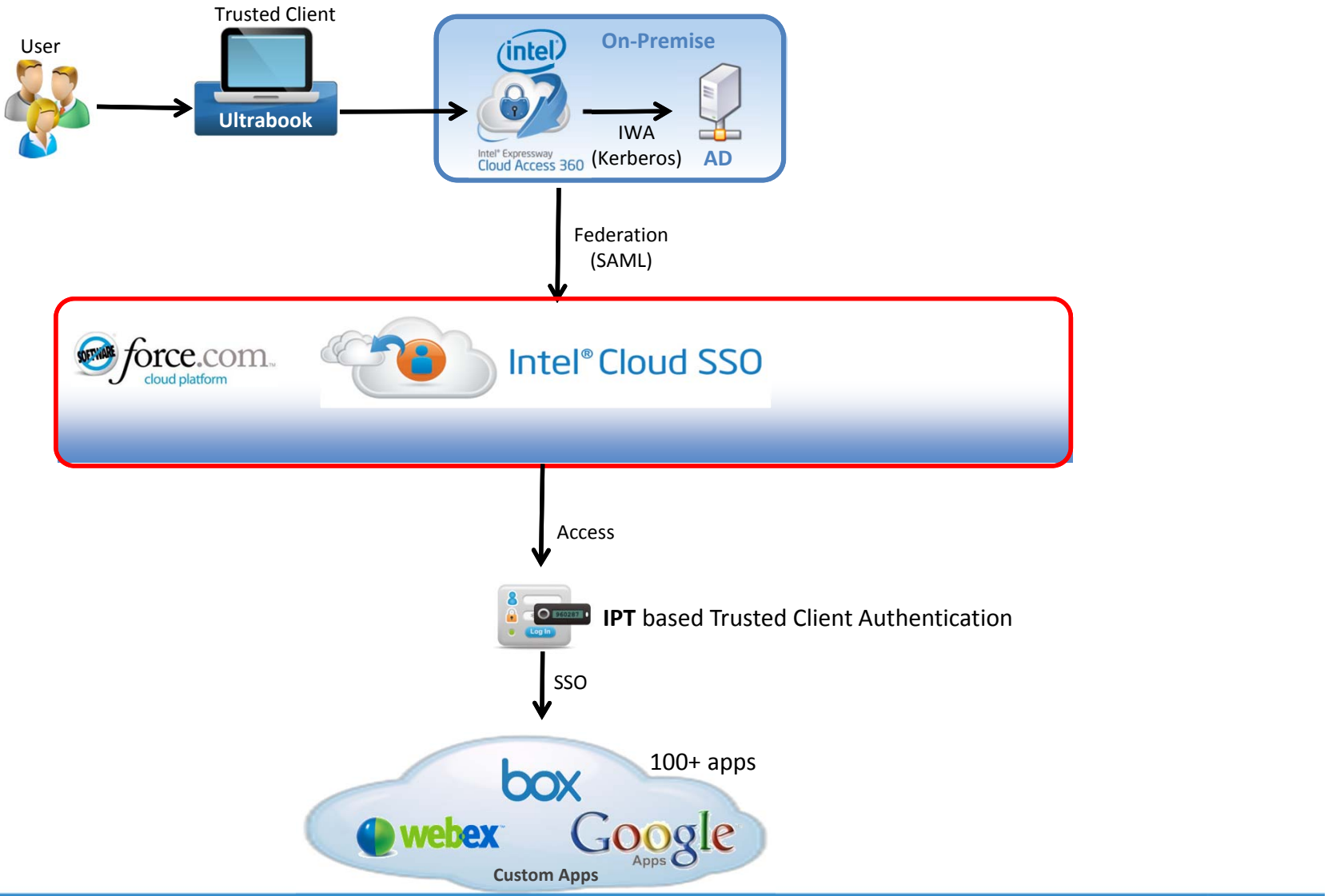
- Delivers same level of control as on-prem IAM
- Leverage Salesforce or enterprise accounts for SSO
- Trigger mobile & hardware assisted strong authentication

Slide 25

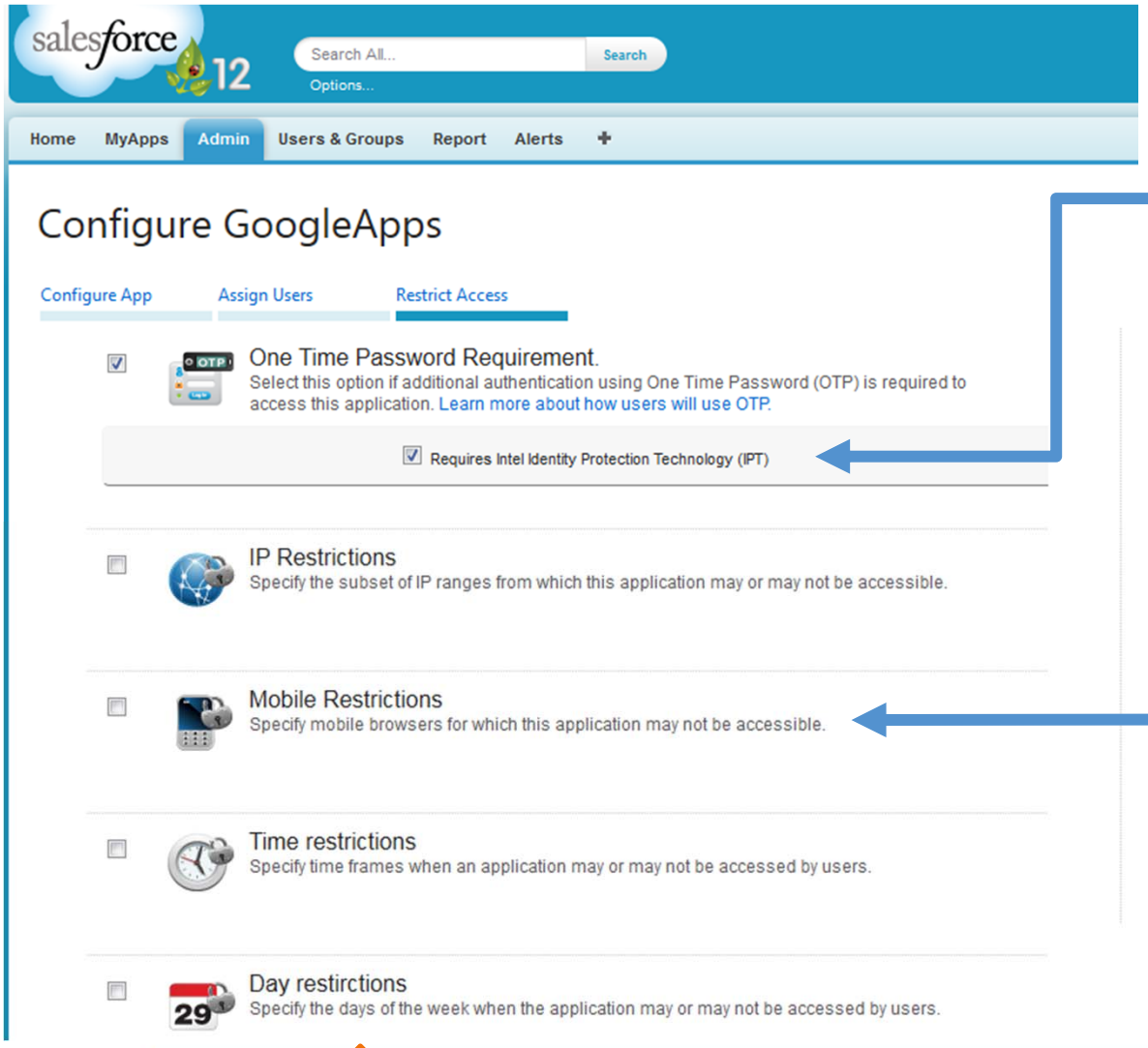
4 new slide to import SSO Portl

Kelly Anderson, 2/17/2012

Demo #2: Trusted Client to Cloud SSO



Unique Context Aware Strong Authentication



Intel Identity Protection Technology
Embedded in 120 million Ultra Books

Fast enrollment mobile OTP

Access Decision

Equip IT with Same Level of On-prem Security Controls

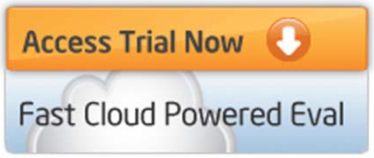
How to Apply What You Have Learned Today

- In the first three months following this presentation you should:
  - Identify all the cloud applications your Enterprise uses
  - Understand how many passwords are being managed
  - Define appropriate compliance controls for events such as a user leaving the company
- Within six months you should:
  - Select an IAM system which allows policy based integrated SSO portal according to your organization's needs
  - Drive an implementation project to secure access to cloud applications

RSACONFERENCE2012

Visit Intel Booth for Demos

www.intelcloudsso.com



Free Trial
April 12

box

Bonus Free Box.net Account

www.intel.com/go/identity

www.mcafee.com/cloudsecurity

Mar 29- Kuppinger Cole Webinar
- How To Outsource Identity to the Cloud

On-Demand Webinar
- Cloud Service Brokers w/CSA & NIST
- Meet the Cloud API w/Forrester Research