Password Less Authentication (PLA)

Srikar Sagi

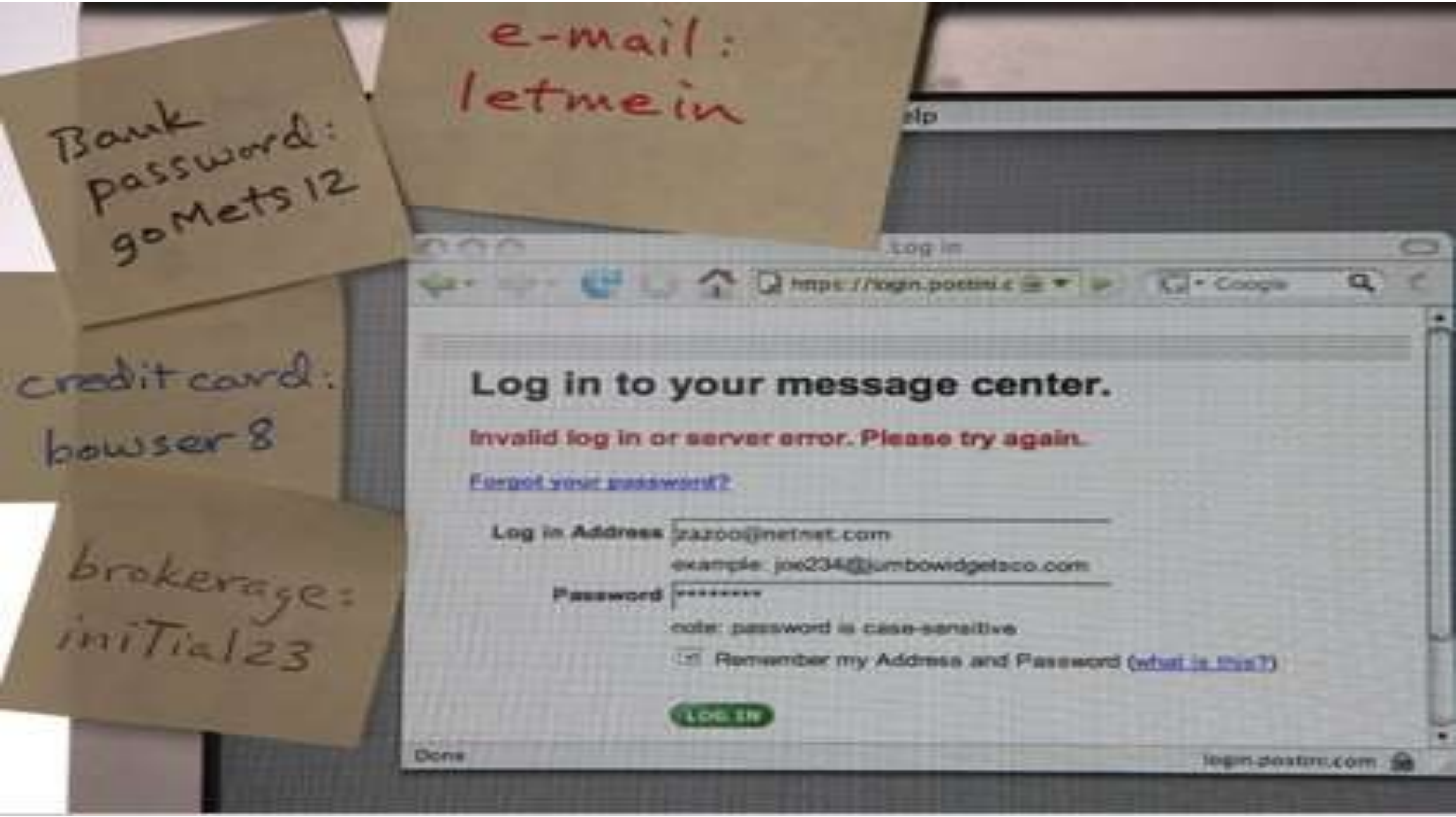
Agenda

- Why Factors - Problem Statement
- Why Factors – Motivations
- Mobile Device based Authentication
- User Registration
- User Experience
- Authentication Process
- Authentication Schematics
- Competitors to PLA
- OTP & PLA Differentiators
- References & QnA
- Appendix

Why Factors-Problem Statements

Customers

Too Many Passwords, password complexities, same passwords, sharing of passwords



Log in to your message center.

Invalid log in or server error. Please try again.

Forgot your password?

Log in Address: zazoo@netnet.com

example: joe234@jumbowidgetsco.com

Password: *********

note: password is case-sensitive

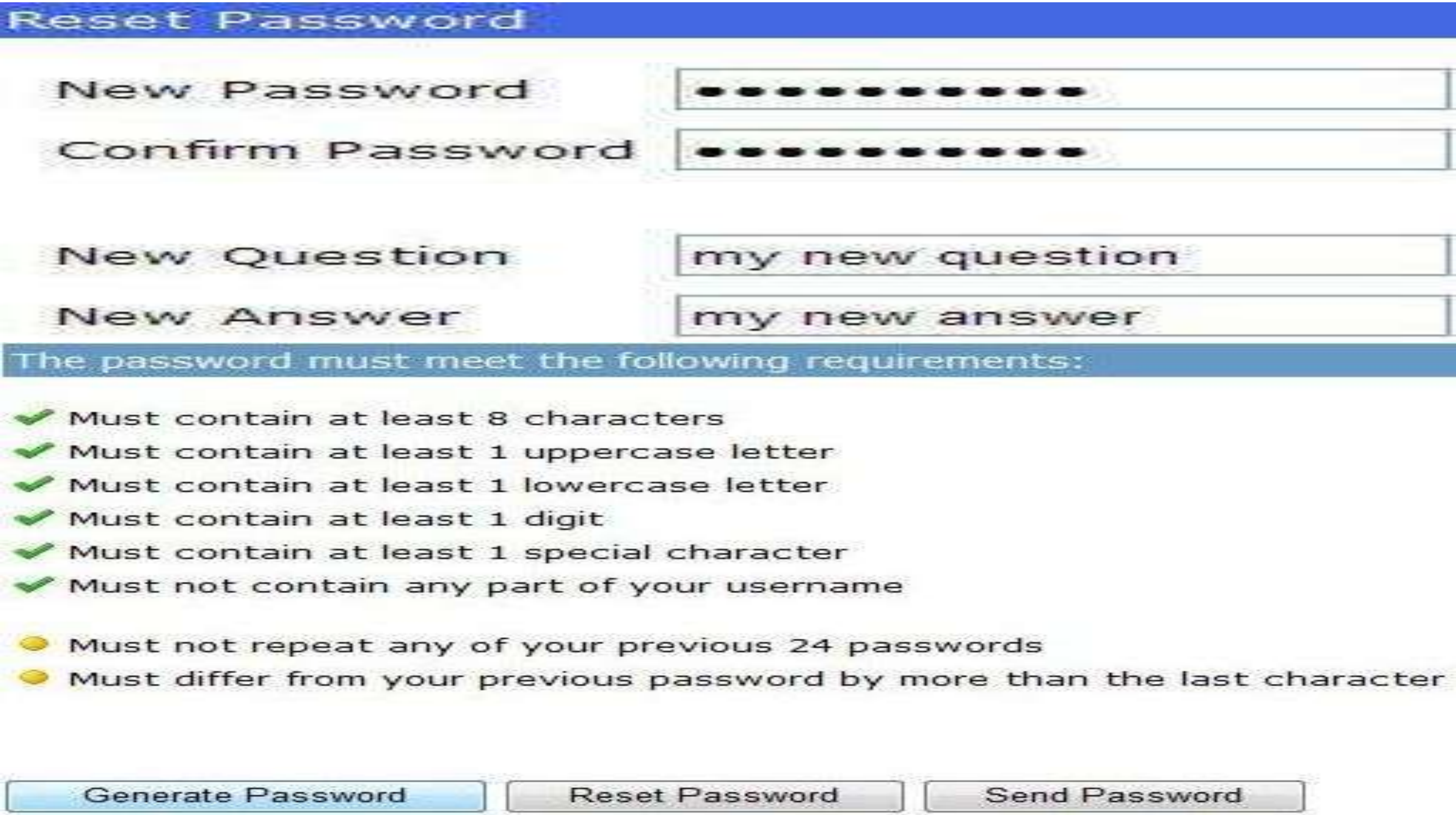
□ Remember my Address and Password (what is this?)

LOG IN

Why Factors-Problem Statements

Customers

Password Changes, Reset requests & Remembering Security Questions for many sites



Reset Password

New Password: •••••••••••••

Confirm Password: •••••••••••••

New Question: my new question

New Answer: my new answer

The password must meet the following requirements:

- ✓ Must contain at least 8 characters
- ✓ Must contain at least 1 uppercase letter
- ✓ Must contain at least 1 lowercase letter
- ✓ Must contain at least 1 digit
- ✓ Must contain at least 1 special character
- ✓ Must not contain any part of your username

- ● Must not repeat any of your previous 24 passwords
- ● Must differ from your previous password by more than the last character

Why Factors-Problem Statements

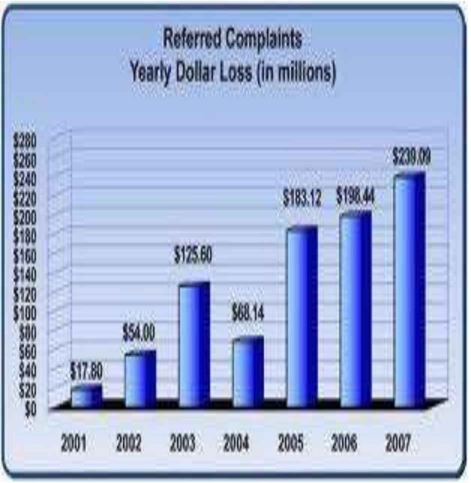
Customers

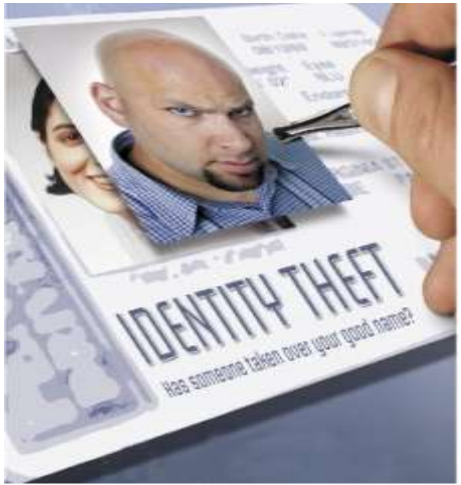
Too many Tokens, Token Costs, Lost Tokens, Dispatch Costs & Lost Business Costs

Why Factors-Problem Statements

Executive Management

- Cost of -- Fraud Operations, Software Security Controls, Service Desk, Frustrated Users & Lost business
- Identity Theft 9.8% (IC3-2010) - 3rd Most Internet Crime
  http://ic3report.nw3c.org/docs/2010_IC3_Report_02_10_11_low_res.pdf
- PoneMon Report – 2011 - Cost of Cyber Crime Study
  http://docs.media.bitpipe.com/io_10x/io_101711/item_452026/2011%202nd%20Annual%20Ponemon%20Cost%20of%20Cybercrime%20Study.pdf
- The Shocking Scale of Cybercrime - Shared by Richard R. in Mobile Security Trends - LinkedIn
  http://www.linkedin.com/news?viewArticle=&articleID=761361820&gid=3802786&type=member&item=69965873&articleURL=http%3A%2F%2Fus.norton.com%2Fcontent%2Fen%2Fus%2Fhome_homeoffice%2Fhtml%2Fcybercrimereport%2F&urlhash=Cjo1&goback=.gde_3802786_member_69965873
- State of Enterprise Security - 2010 Report by Norton
  http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf

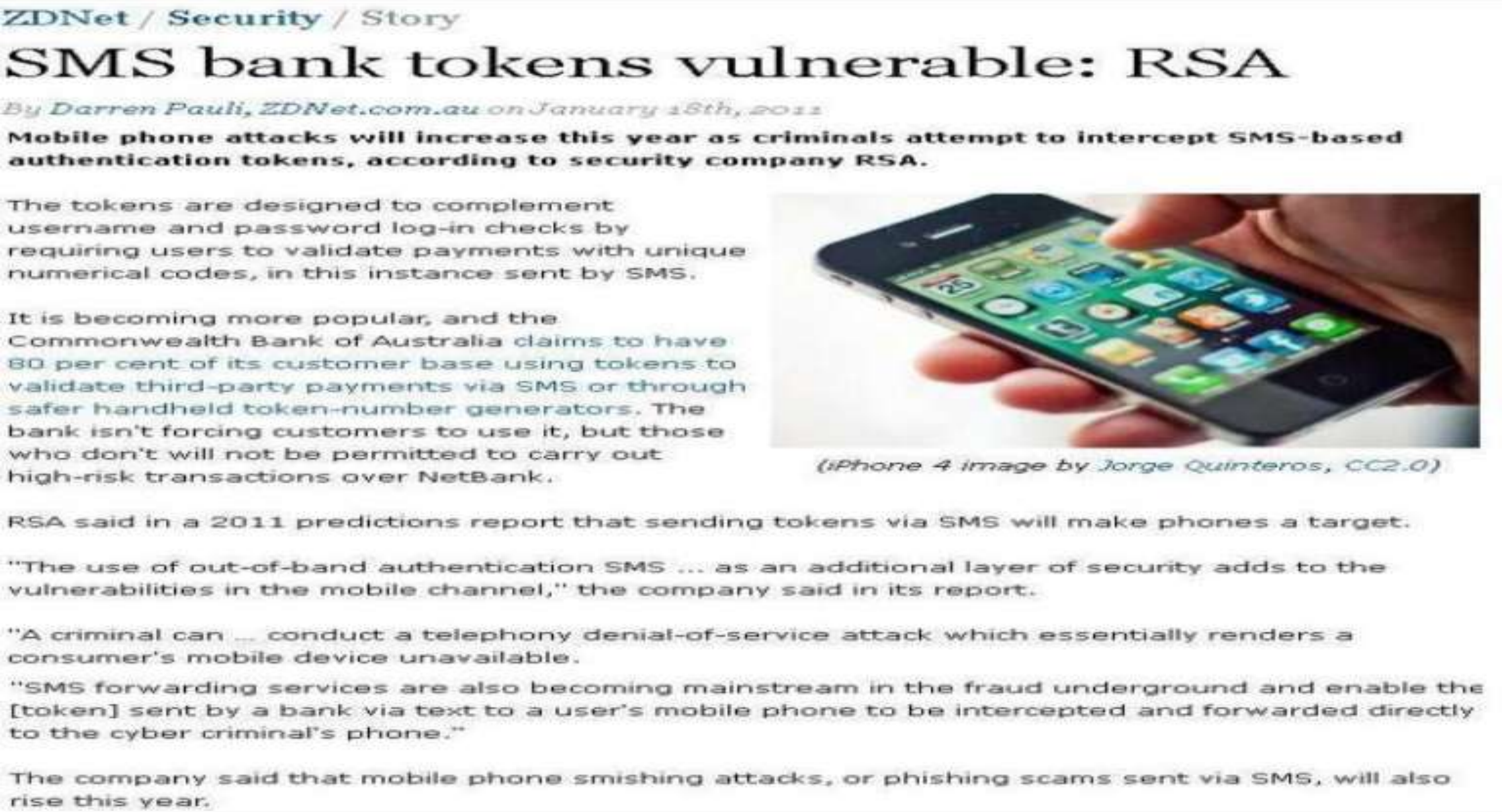




Why Factors-Motivation

SMS Bank Tokens Vulnerable

http://www.zdnet.com.au/sms-bank-tokens-vulnerable-rsa-339308633.htm



ZDNet / Security / Story

SMS bank tokens vulnerable: RSA

By Darren Pauli, ZDNet.com.au on January 18th, 2011

Mobile phone attacks will increase this year as criminals attempt to intercept SMS-based authentication tokens, according to security company RSA.

The tokens are designed to complement username and password log-in checks by requiring users to validate payments with unique numerical codes, in this instance sent by SMS.

It is becoming more popular, and the Commonwealth Bank of Australia claims to have 80 per cent of its customer base using tokens to validate third-party payments via SMS or through safer handheld token-number generators. The bank isn't forcing customers to use it, but those who don't will not be permitted to carry out high-risk transactions over NetBank.

(iPhone 4 image by Jorge Quinteros, CC2.0)

RSA said in a 2011 predictions report that sending tokens via SMS will make phones a target.

"The use of out-of-band authentication SMS ... as an additional layer of security adds to the vulnerabilities in the mobile channel," the company said in its report.

"A criminal can ... conduct a telephony denial-of-service attack which essentially renders a consumer's mobile device unavailable.

"SMS forwarding services are also becoming mainstream in the fraud underground and enable the [token] sent by a bank via text to a user's mobile phone to be intercepted and forwarded directly to the cyber criminal's phone."

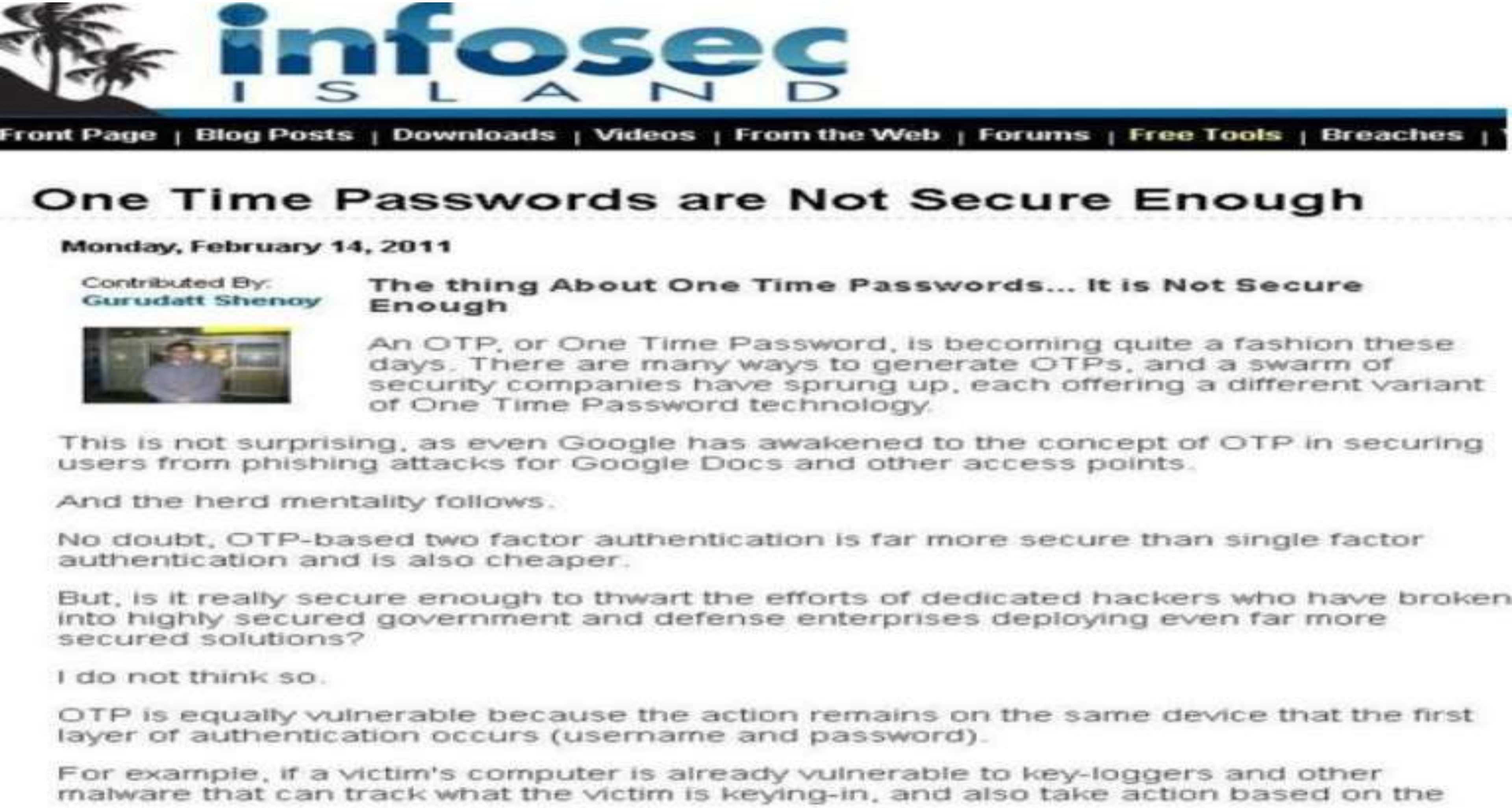
The company said that mobile phone smishing attacks, or phishing scams sent via SMS, will also rise this year.

Why Factors-Motivation

One Time Passwords are not Secure – Analysis

https://infosecisland.com/blogview/11813-One-Time-Passwords-are-Not-Secure-Enough.html

http://www.nowires.org/Papers-PDF/OTPanalysis.pdf


infosec ISLAND
Front Page | Blog Posts | Downloads | Videos | From the Web | Forums | Free Tools | Breaches |

One Time Passwords are Not Secure Enough

Monday, February 14, 2011

Contributed By:
Gurudatt Shenoy

The thing About One Time Passwords... It is Not Secure Enough

An OTP, or One Time Password, is becoming quite a fashion these days. There are many ways to generate OTPs, and a swarm of security companies have sprung up, each offering a different variant of One Time Password technology.

This is not surprising, as even Google has awakened to the concept of OTP in securing users from phishing attacks for Google Docs and other access points.

And the herd mentality follows.

No doubt, OTP-based two factor authentication is far more secure than single factor authentication and is also cheaper.

But, is it really secure enough to thwart the efforts of dedicated hackers who have broken into highly secured government and defense enterprises deploying even far more secured solutions?

I do not think so.

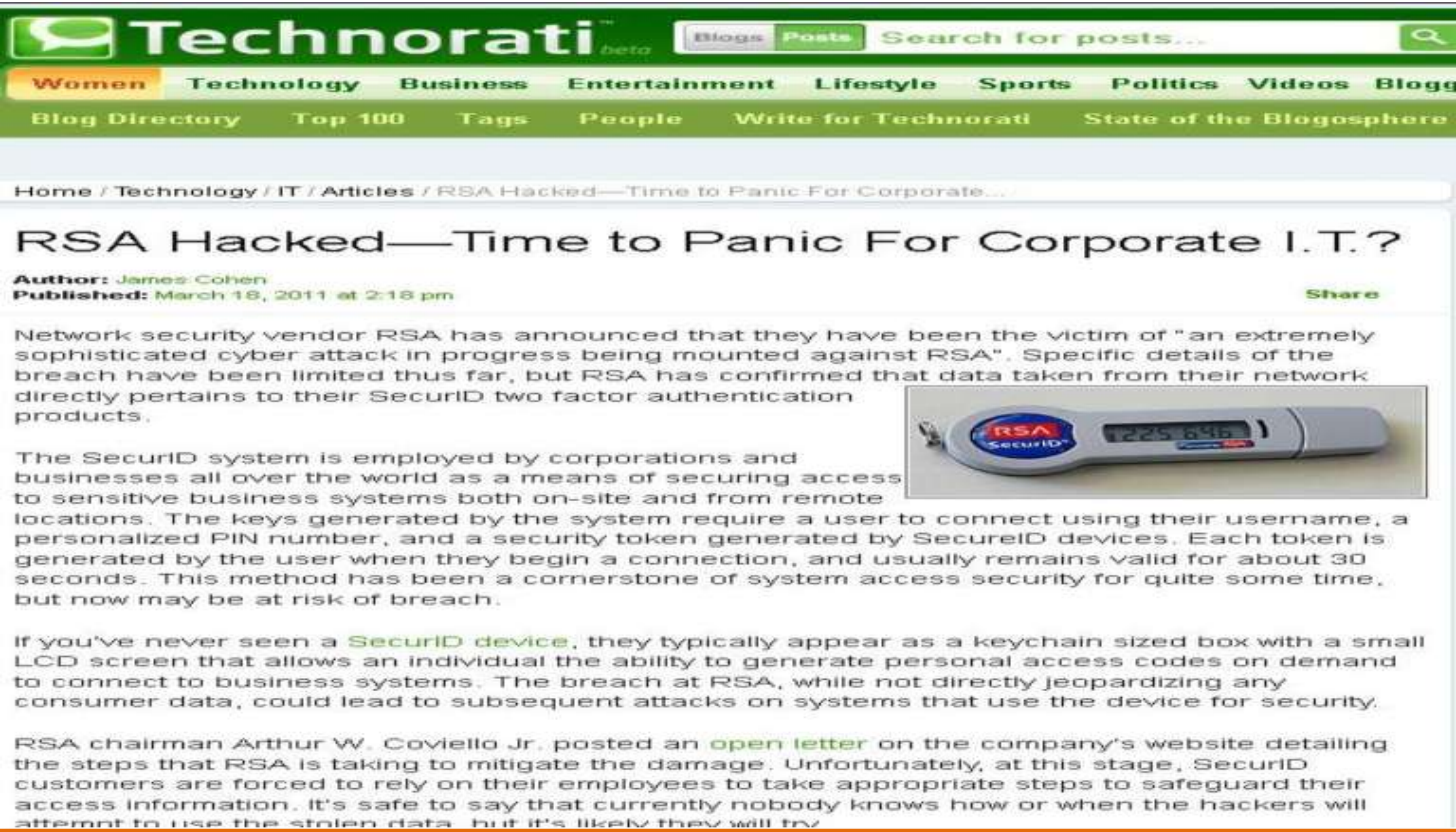
OTP is equally vulnerable because the action remains on the same device that the first layer of authentication occurs (username and password).

For example, if a victim's computer is already vulnerable to key-loggers and other malware that can track what the victim is keying-in, and also take action based on the

Why Factors-Motivation

RSA Secure-ID Hardware Token Hacked

http://technorati.com/technology/it/article/rsa-hackedtime-to-panic-for-corporate/



RSA Hacked—Time to Panic For Corporate I.T.?

Author: James Cohen
Published: March 18, 2011 at 2:18 pm

Network security vendor RSA has announced that they have been the victim of "an extremely sophisticated cyber attack in progress being mounted against RSA". Specific details of the breach have been limited thus far, but RSA has confirmed that data taken from their network directly pertains to their SecurID two factor authentication products.

The SecurID system is employed by corporations and businesses all over the world as a means of securing access to sensitive business systems both on-site and from remote locations. The keys generated by the system require a user to connect using their username, a personalized PIN number, and a security token generated by SecureID devices. Each token is generated by the user when they begin a connection, and usually remains valid for about 30 seconds. This method has been a cornerstone of system access security for quite some time, but now may be at risk of breach.

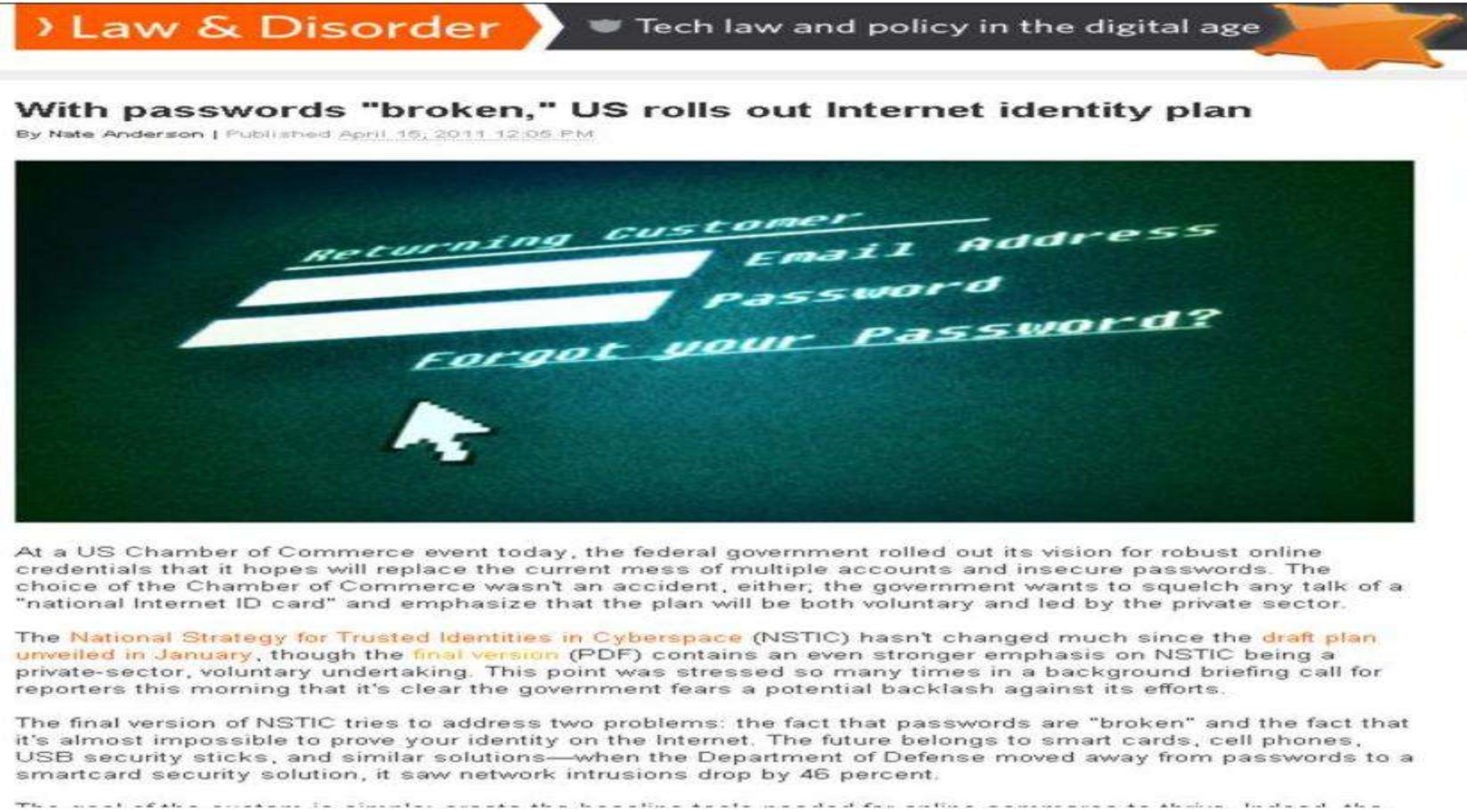
If you've never seen a SecurID device, they typically appear as a keychain sized box with a small LCD screen that allows an individual the ability to generate personal access codes on demand to connect to business systems. The breach at RSA, while not directly jeopardizing any consumer data, could lead to subsequent attacks on systems that use the device for security.

RSA chairman Arthur W. Coviello Jr. posted an open letter on the company's website detailing the steps that RSA is taking to mitigate the damage. Unfortunately, at this stage, SecurID customers are forced to rely on their employees to take appropriate steps to safeguard their access information. It's safe to say that currently nobody knows how or when the hackers will attempt to use the stolen data, but it's likely they will try.

Why Factors-Motivation

US Chamber of Commerce – Proposing No Passwords, Only H/W or Smart Phone based Login

http://arstechnica.com/tech-policy/news/2011/04/with-passwords-broken-us-rolls-out-internet-identity-plan.ars



With passwords "broken," US rolls out Internet identity plan

By Nate Anderson | Published April 15, 2011 12:05 PM

At a US Chamber of Commerce event today, the federal government rolled out its vision for robust online credentials that it hopes will replace the current mess of multiple accounts and insecure passwords. The choice of the Chamber of Commerce wasn't an accident, either; the government wants to squelch any talk of a "national Internet ID card" and emphasize that the plan will be both voluntary and led by the private sector.

The National Strategy for Trusted Identities in Cyberspace (NSTIC) hasn't changed much since the draft plan unveiled in January, though the final version (PDF) contains an even stronger emphasis on NSTIC being a private-sector, voluntary undertaking. This point was stressed so many times in a background briefing call for reporters this morning that it's clear the government fears a potential backlash against its efforts.

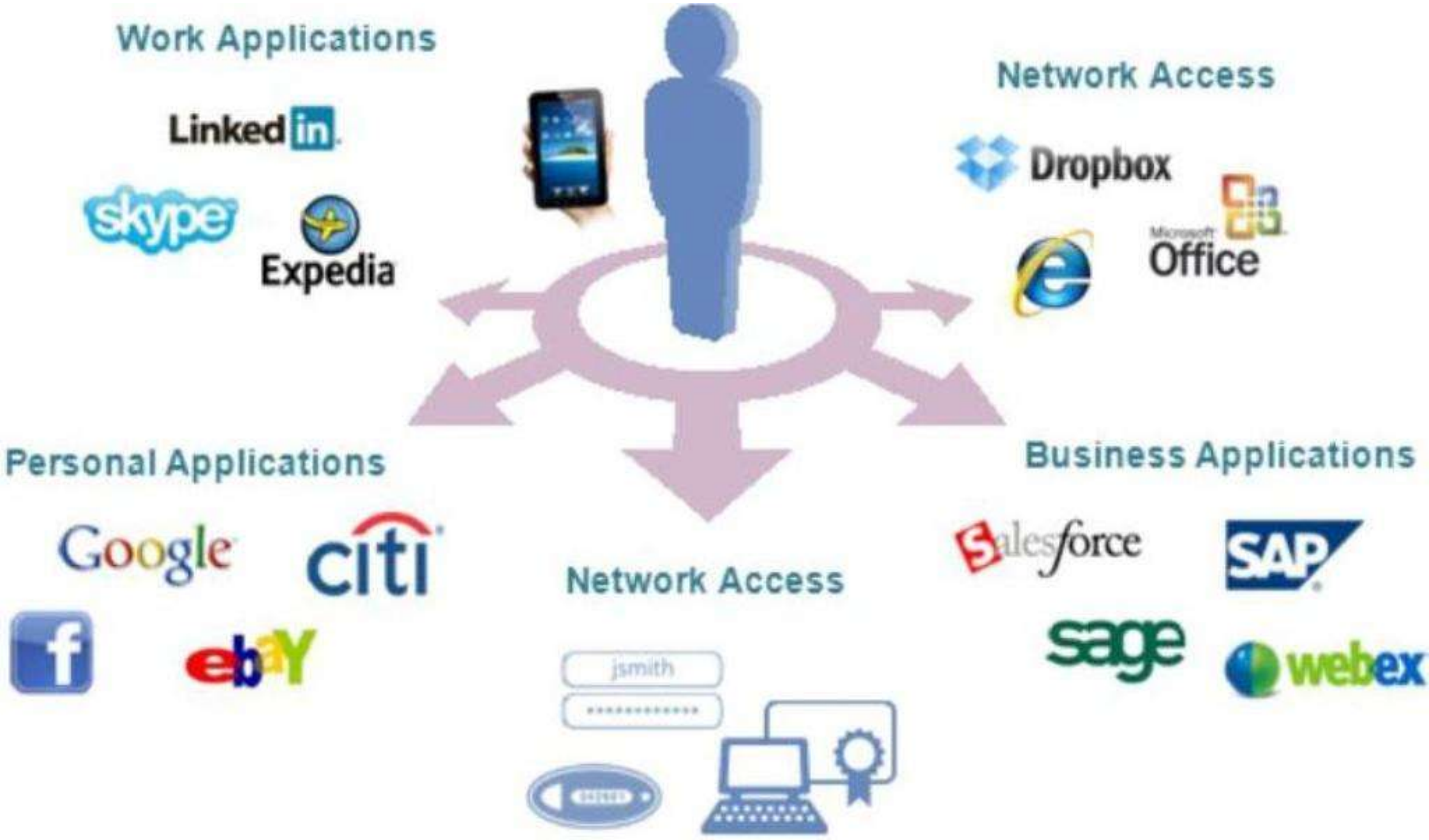
The final version of NSTIC tries to address two problems: the fact that passwords are "broken" and the fact that it's almost impossible to prove your identity on the Internet. The future belongs to smart cards, cell phones, USB security sticks, and similar solutions—when the Department of Defense moved away from passwords to a smartcard security solution, it saw network intrusions drop by 46 percent.

The goal of the system is simple: create the baseline tools needed for online commerce to thrive. Indeed, the

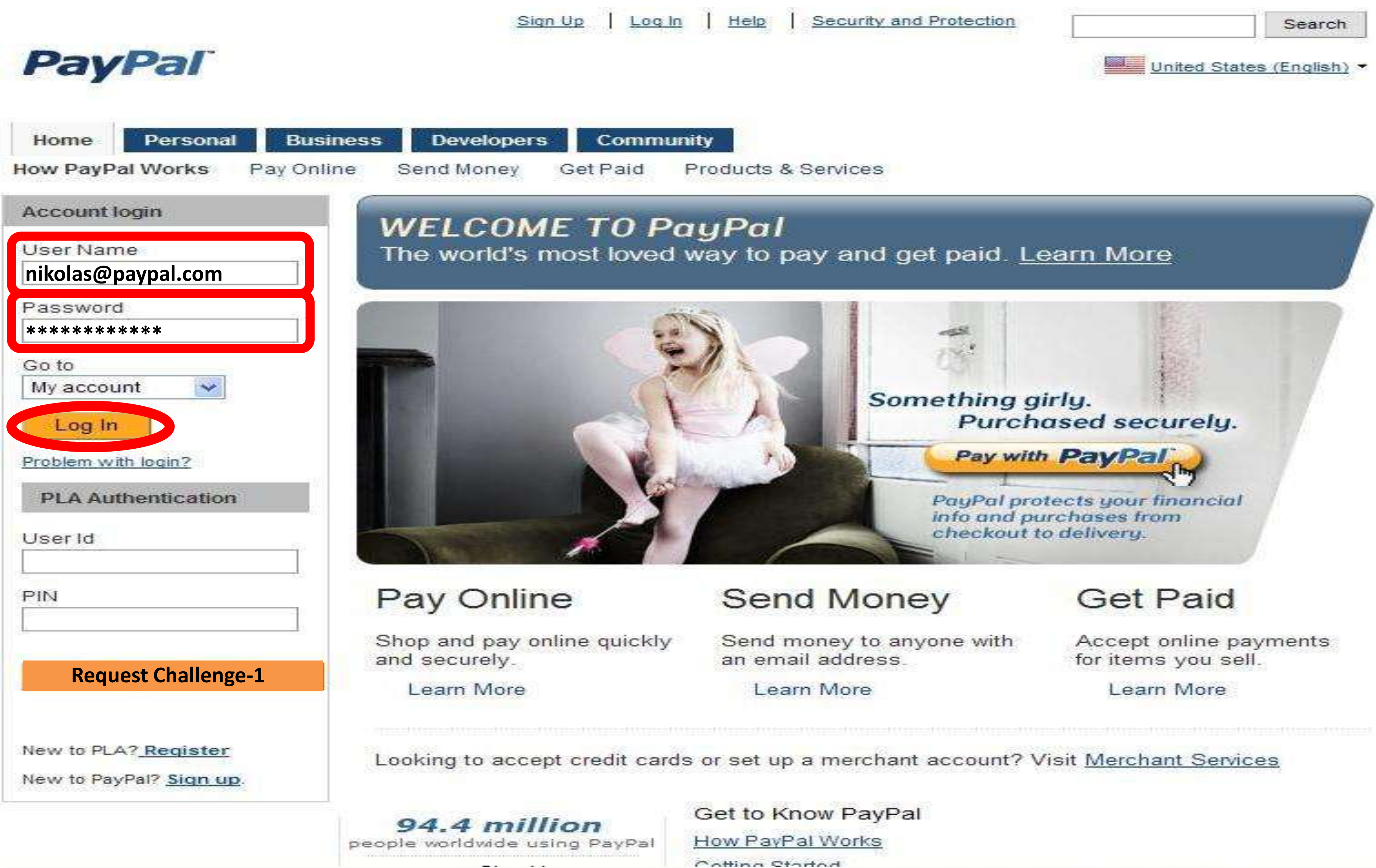
Why Factors-Motivation

- Human *Psyche* for Mobile phones
- Frustrated Users – many & similar Passwords
- Human Dependency on Mobile phones
- Trust on Mobile Network’s Control Channel
- Increase in Mobile Device Capabilities
- Use of Mobile’s Geo Loc’ for Authorization Decision
- Trust on Public Key Cryptography
- Automated Mobile Signal attacks are costly (Logistics)
- Mobile Apps – Controlled by Central Release Authorities
- Mobile Phone Population crossing 5 Billion devices
- Adult(15-65)Population more than 3 Billion out of 7 Billion
- Expected – 50 Billion Internet connected Devices by 2020

Mobile Device based Authentication



User Registration



Account login

User Name: nikolas@paypal.com

Password: ************

Go to: My account

Log In

Problem with login?

PLA Authentication

User Id:

PIN:

Request Challenge-1

New to PLA? Register

New to PayPal? Sign up.

WELCOME TO PayPal

The world's most loved way to pay and get paid. Learn More

Something girly. Purchased securely.

Pay with PayPal

PayPal protects your financial info and purchases from checkout to delivery.

Pay Online

Shop and pay online quickly and securely.

Learn More

Send Money

Send money to anyone with an email address.

Learn More

Get Paid

Accept online payments for items you sell.

Learn More

Looking to accept credit cards or set up a merchant account? Visit Merchant Services

94.4 million

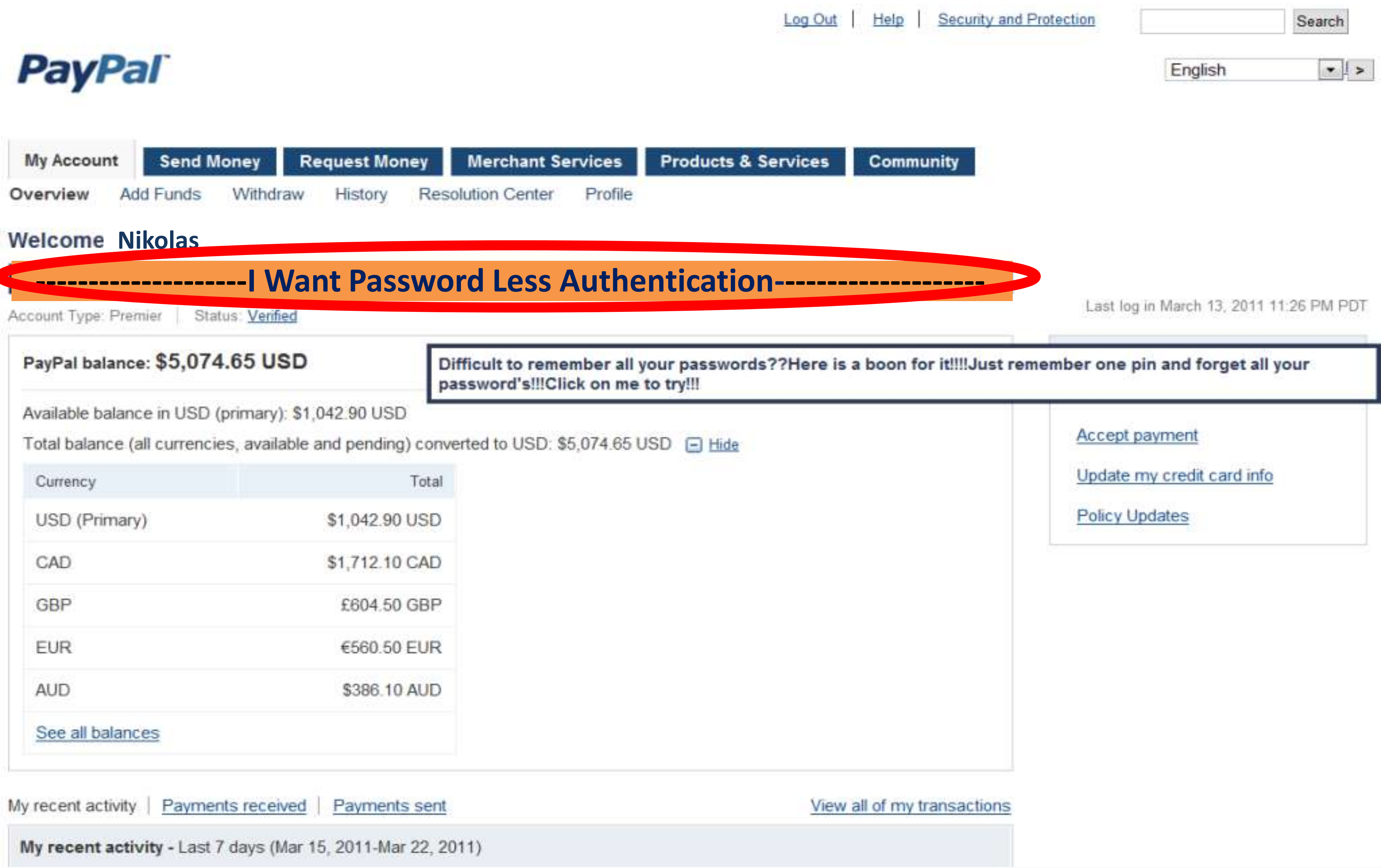
people worldwide using PayPal

Get to Know PayPal

How PayPal Works

Getting Started

User Registration



Log Out | Help | Security and Protection

Search

PayPal

English

My Account | Send Money | Request Money | Merchant Services | Products & Services | Community

Overview | Add Funds | Withdraw | History | Resolution Center | Profile

Welcome Nikolas

-------------------I Want Password Less Authentication-------------------

Account Type: Premier | Status: Verified

Last log in March 13, 2011 11:26 PM PDT

Difficult to remember all your passwords??Here is a boon for it!!!!Just remember one pin and forget all your password's!!!Click on me to try!!!

PayPal balance: $5,074.65 USD

Available balance in USD (primary): $1,042.90 USD

Total balance (all currencies, available and pending) converted to USD: $5,074.65 USD ⊟ Hide

Currency	Total
USD (Primary)	$1,042.90 USD
CAD	$1,712.10 CAD
GBP	£604.50 GBP
EUR	€560.50 EUR
AUD	$386.10 AUD

See all balances

Accept payment

Update my credit card info

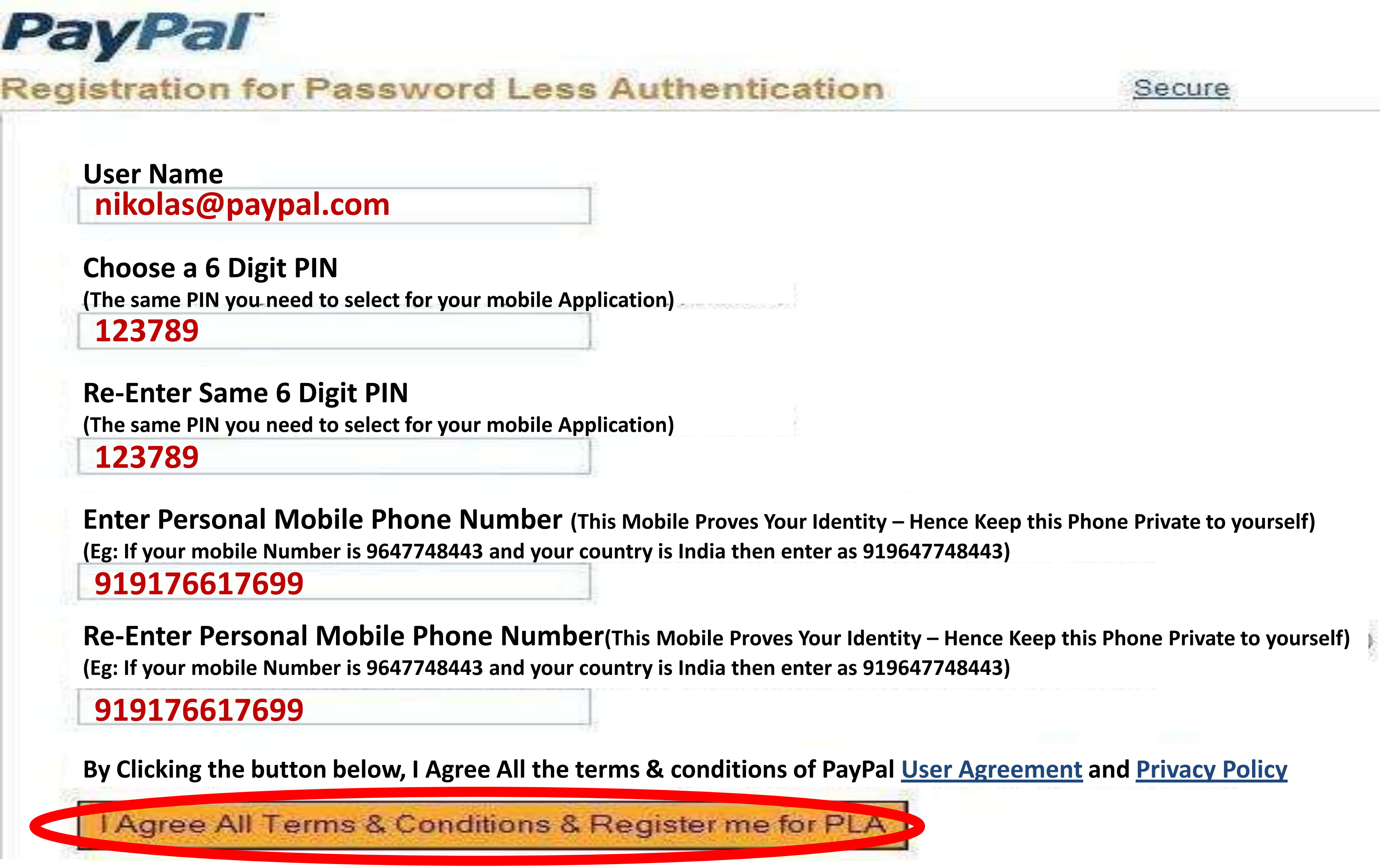
Policy Updates

My recent activity | Payments received | Payments sent

View all of my transactions

My recent activity - Last 7 days (Mar 15, 2011-Mar 22, 2011)

User Registration



PayPal

Registration for Password Less Authentication

User Name
nikolas@paypal.com

Choose a 6 Digit PIN
(The same PIN you need to select for your mobile Application)
123789

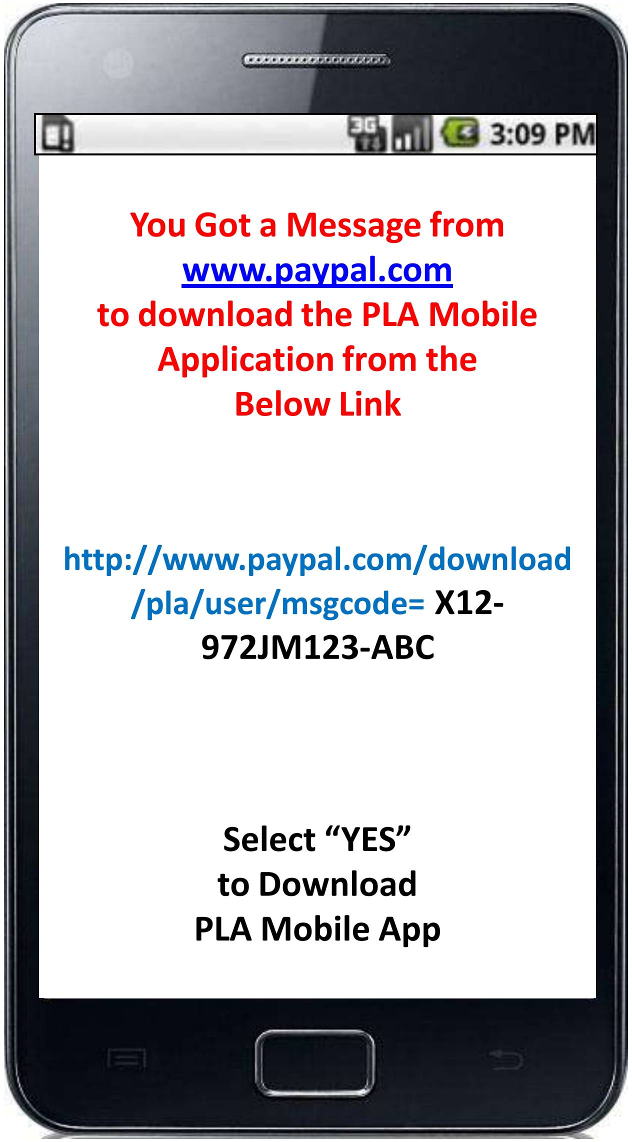
Re-Enter Same 6 Digit PIN
(The same PIN you need to select for your mobile Application)
123789

Enter Personal Mobile Phone Number (This Mobile Proves Your Identity – Hence Keep this Phone Private to yourself)
(Eg: If your mobile Number is 9647748443 and your country is India then enter as 919647748443)
919176617699

Re-Enter Personal Mobile Phone Number(This Mobile Proves Your Identity – Hence Keep this Phone Private to yourself)
(Eg: If your mobile Number is 9647748443 and your country is India then enter as 919647748443)
919176617699

By Clicking the button below, I Agree All the terms & conditions of PayPal User Agreement and Privacy Policy

User Registration



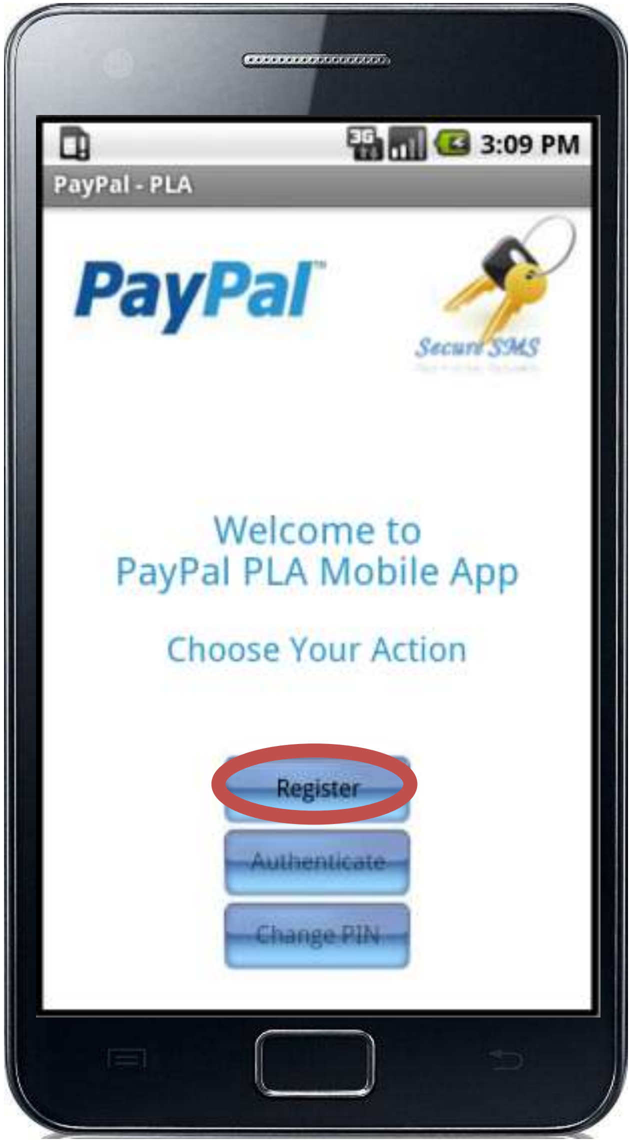
3:09 PM

You Got a Message from
www.paypal.com
to download the PLA Mobile
Application from the
Below Link

http://www.paypal.com/download
/pla/user/msgcode= X12-
972JM123-ABC

Select “YES”
to Download
PLA Mobile App

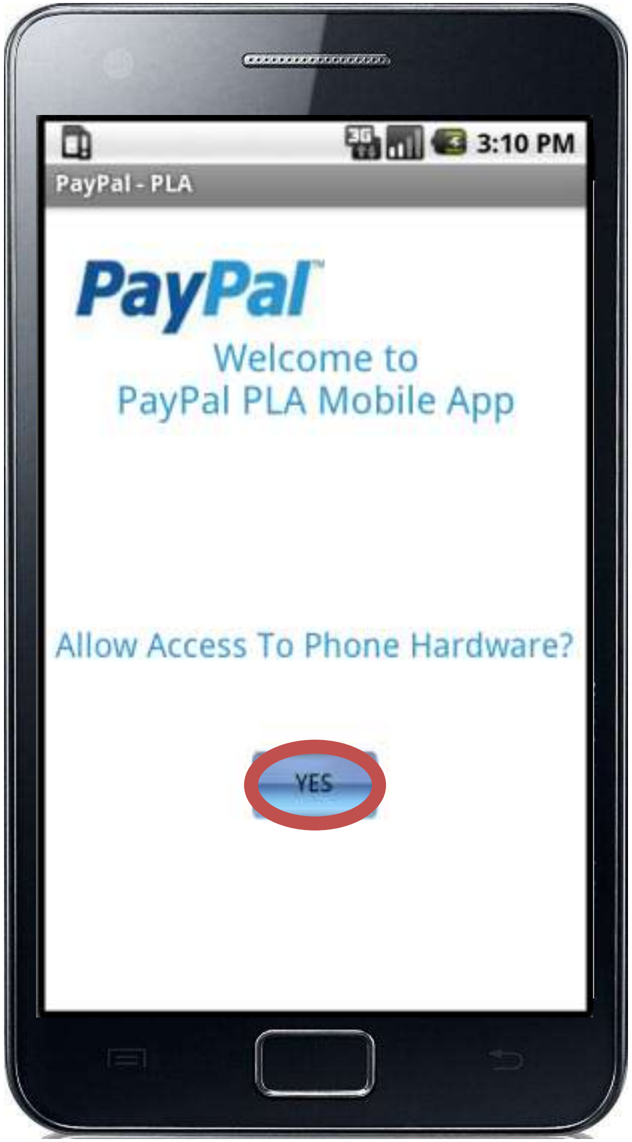
User Registration



Welcome to
PayPal PLA Mobile App

Choose Your Action

User Registration



3:10 PM

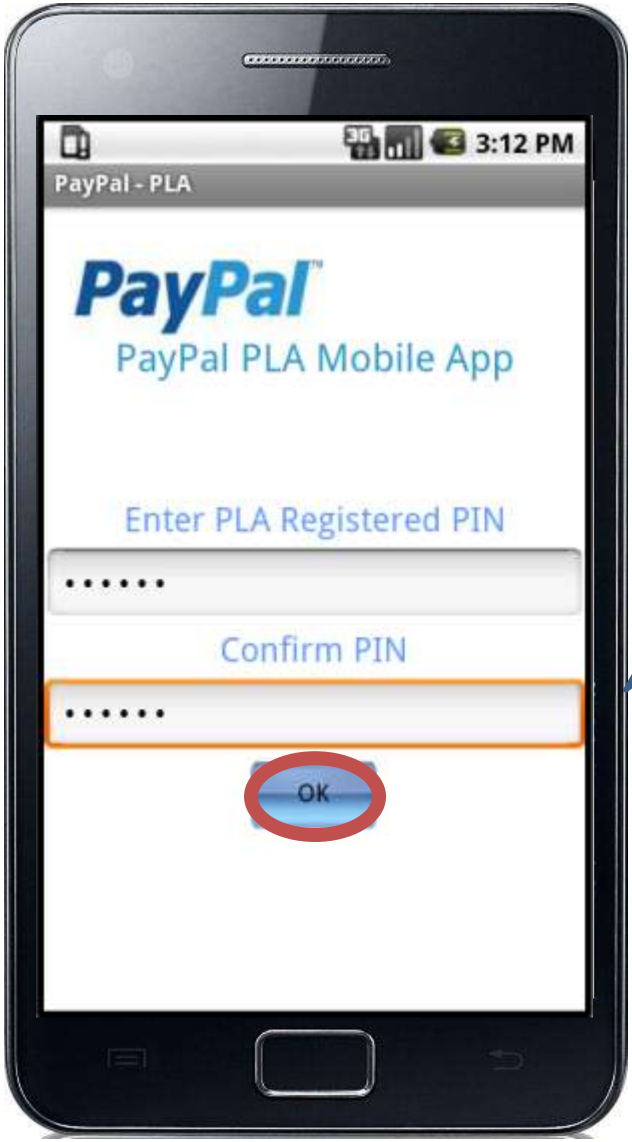
PayPal - PLA

Welcome to
PayPal PLA Mobile App

Allow Access To Phone Hardware?

To read
IMSI &
ICC-ID

User Registration



3:12 PM

PayPal - PLA

PayPal

PayPal PLA Mobile App

Enter PLA Registered PIN

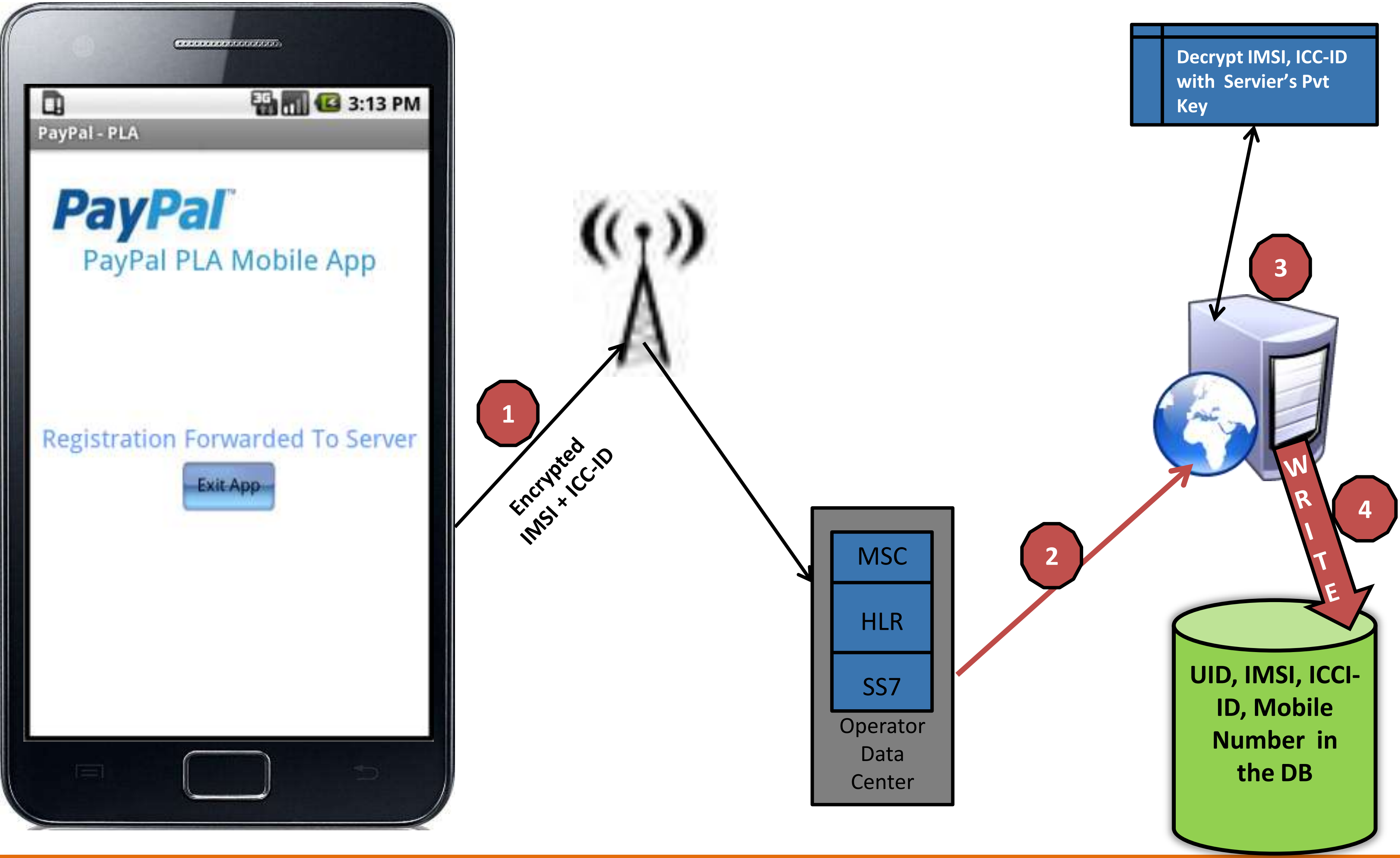
••••••

Confirm PIN

••••••

Same PIN Entered on the web page

User Registration



1 Encrypted IMSI + ICC-ID

MSC

HLR

SS7

Operator Data Center

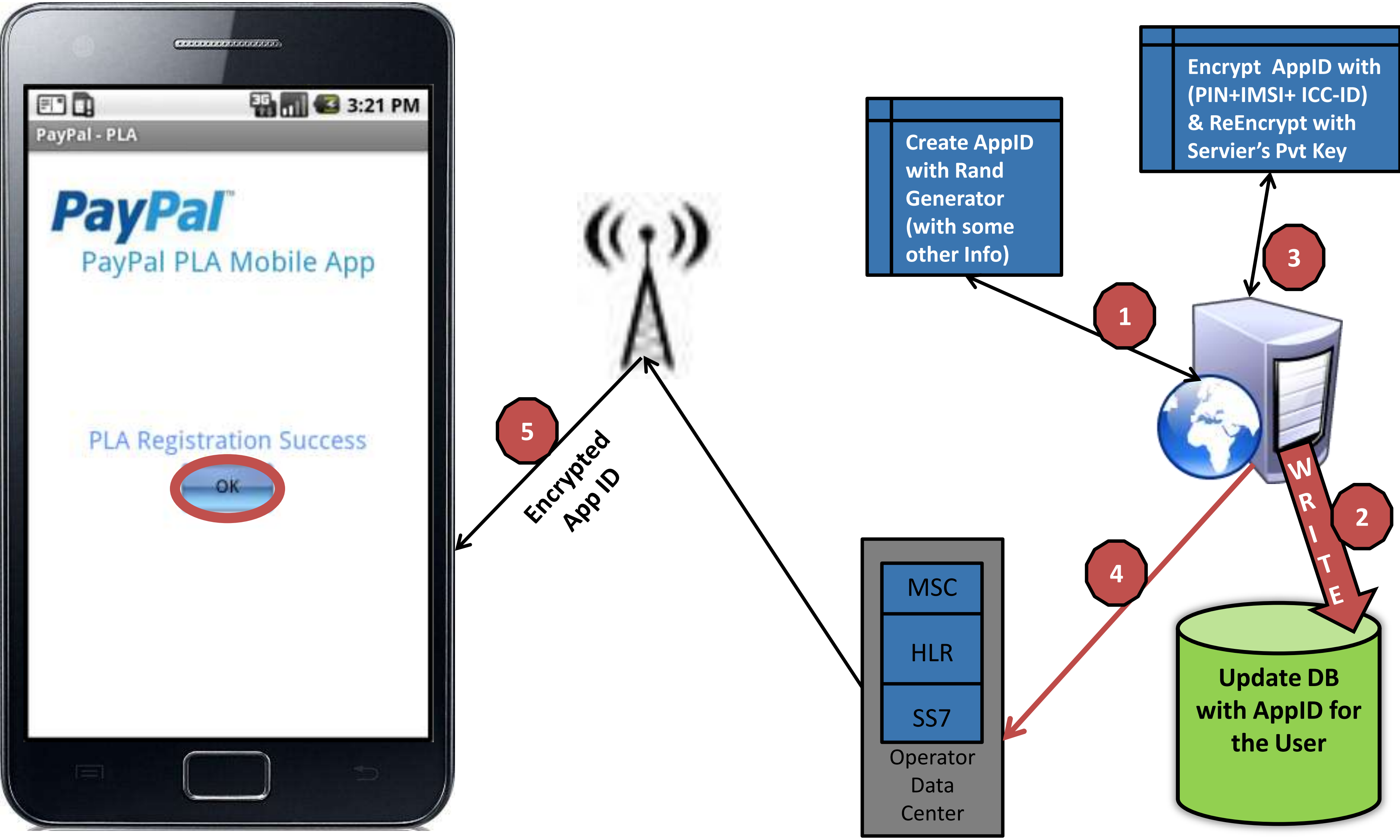
2

3 Decrypt IMSI, ICC-ID with Servier's Pvt Key

4 WRITE

UID, IMSI, ICCI-ID, Mobile Number in the DB

User Registration

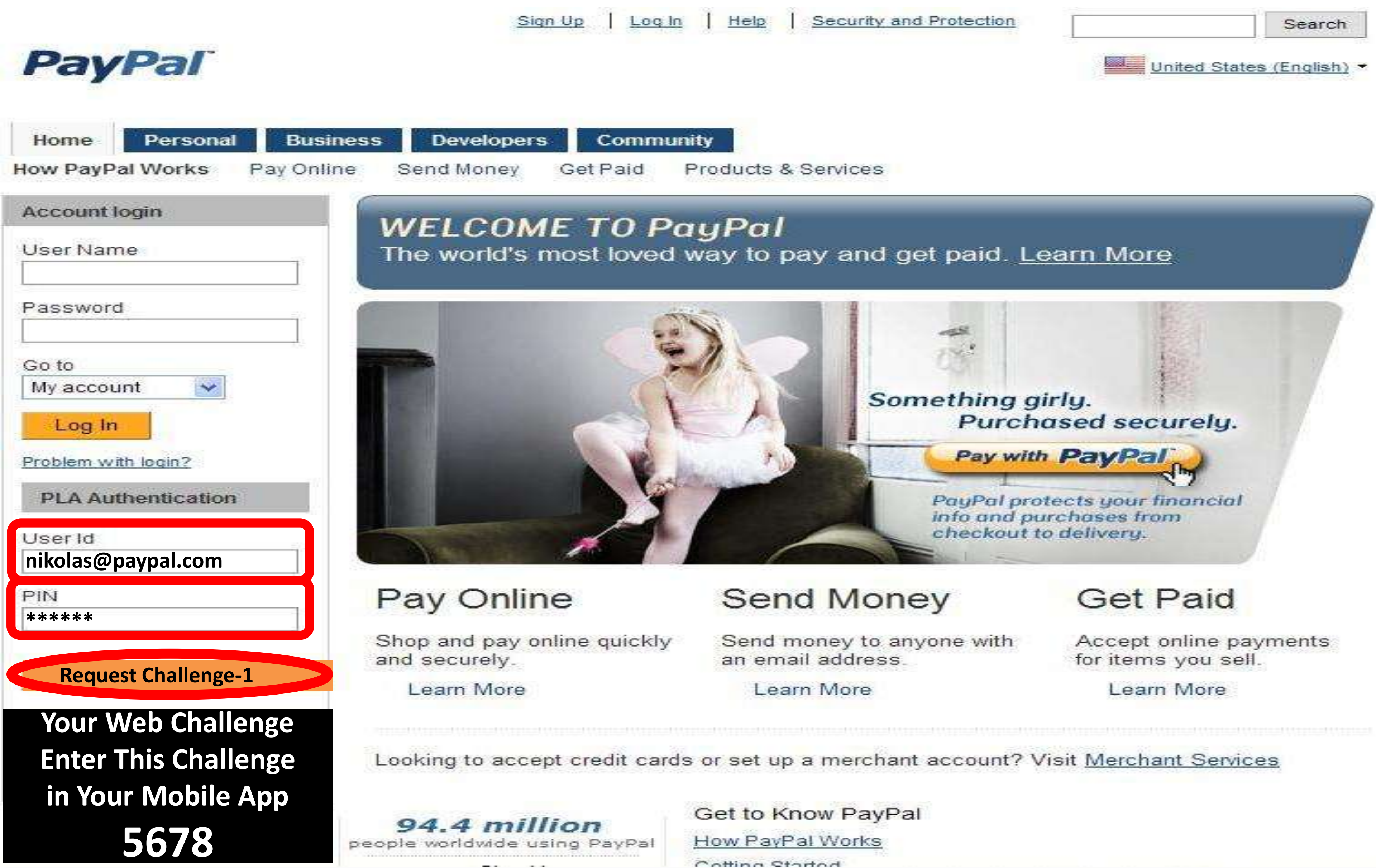


Create AppID with Rand Generator (with some other Info)

Encrypt AppID with (PIN+IMSI+ ICC-ID) & ReEncrypt with Servier's Pvt Key

Update DB with AppID for the User

User Experience



Sign Up | Log In | Help | Security and Protection

Search

PayPal

United States (English)

Home | Personal | Business | Developers | Community

How PayPal Works | Pay Online | Send Money | Get Paid | Products & Services

Account login

User Name

Password

Go to

My account

Log In

Problem with login?

PLA Authentication

User Id

nikolas@paypal.com

PIN

******

Request Challenge-1

Your Web Challenge
Enter This Challenge
in Your Mobile App
5678

WELCOME TO PayPal

The world's most loved way to pay and get paid. Learn More

Something girly.
Purchased securely.
Pay with PayPal
PayPal protects your financial info and purchases from checkout to delivery.

Pay Online

Shop and pay online quickly and securely.

Learn More

Send Money

Send money to anyone with an email address.

Learn More

Get Paid

Accept online payments for items you sell.

Learn More

Looking to accept credit cards or set up a merchant account? Visit Merchant Services

94.4 million

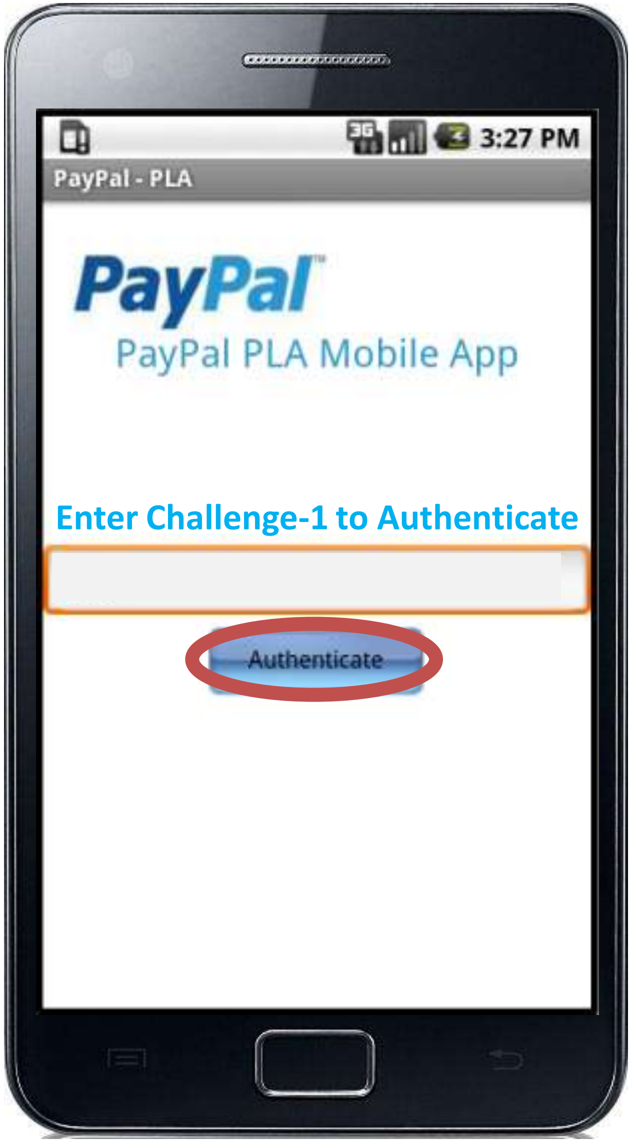
people worldwide using PayPal

Get to Know PayPal

How PayPal Works

Getting Started

User Experience



3:27 PM

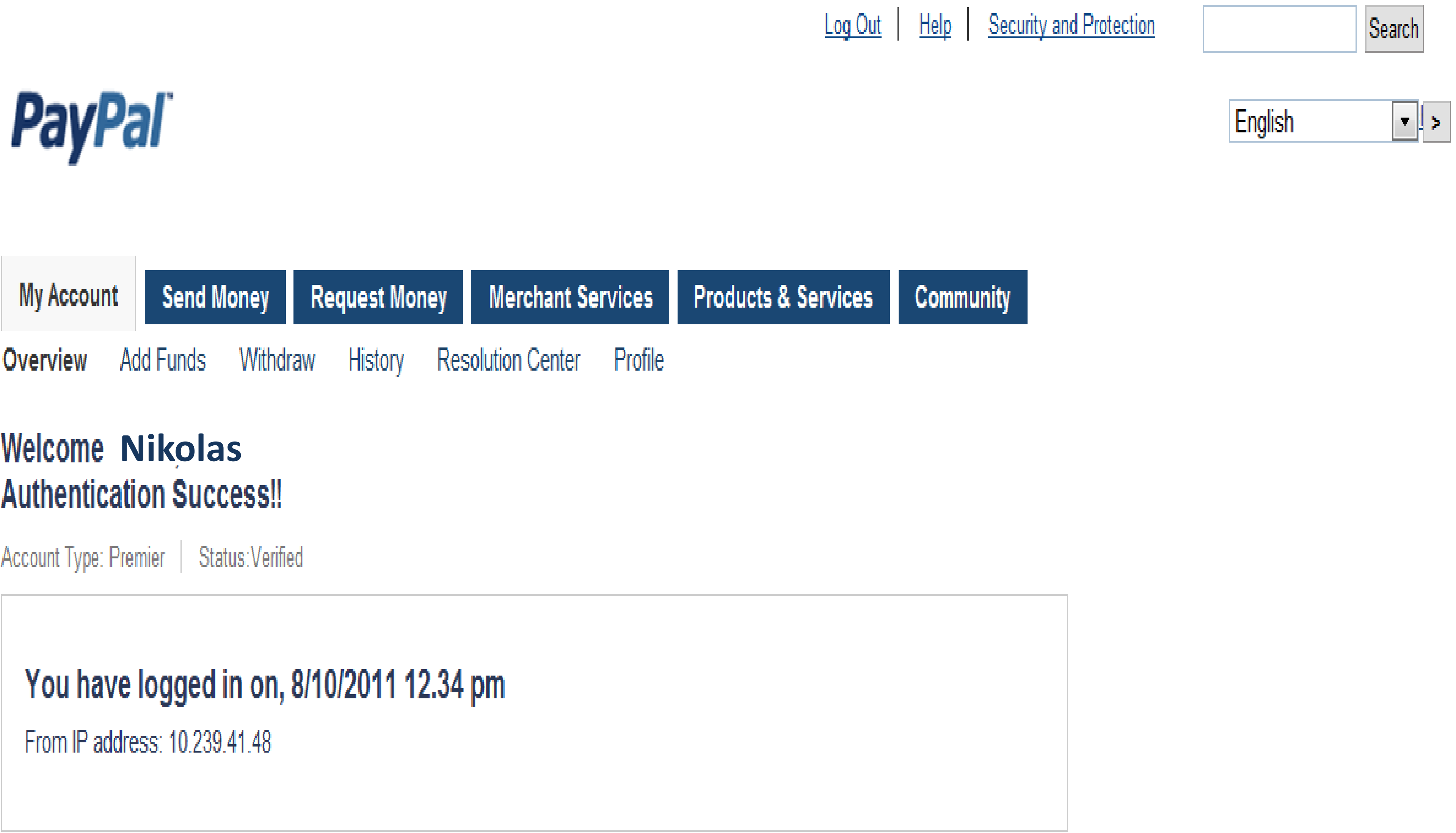
PayPal - PLA

PayPal

PayPal PLA Mobile App

Enter Challenge-1 to Authenticate

User Experience



Welcome Nikolas

Authentication Success!!

Account Type: Premier | Status:Verified

You have logged in on, 8/10/2011 12.34 pm

From IP address: 10.239.41.48

Authentication Process

Step-1 Credential Collection on ***TWO distinct*** Networks

Step-2 User ID is sent by User as ***multipart/x-mixed-replace*** Request
and ***Challenge-1*** is received on Web Page from Server
on IP Network as a multipart/x-mixed-replace Response

Step-3 Server Sends ***Challenge-2*** as Push/SMS Message on Mobile
Phone over the air using Telecom Network (stores Challenge-1 & 2)

Step-4 User enters ***Challenge-1*** on Mobile App & Mobile App reads
Challenge-2 from Push/SMS, Hashes ***C1+C2+IMSI+ICC-ID+AppID***
and Encrypts with Server's Public Key (Encrypted Packet)

NOTE: ***Challenge-2*** is always Opaque to user– may or may not know

Authentication Process

Step-5 Encrypted Packet is Sent as SMS/Push Response from Mobile Network

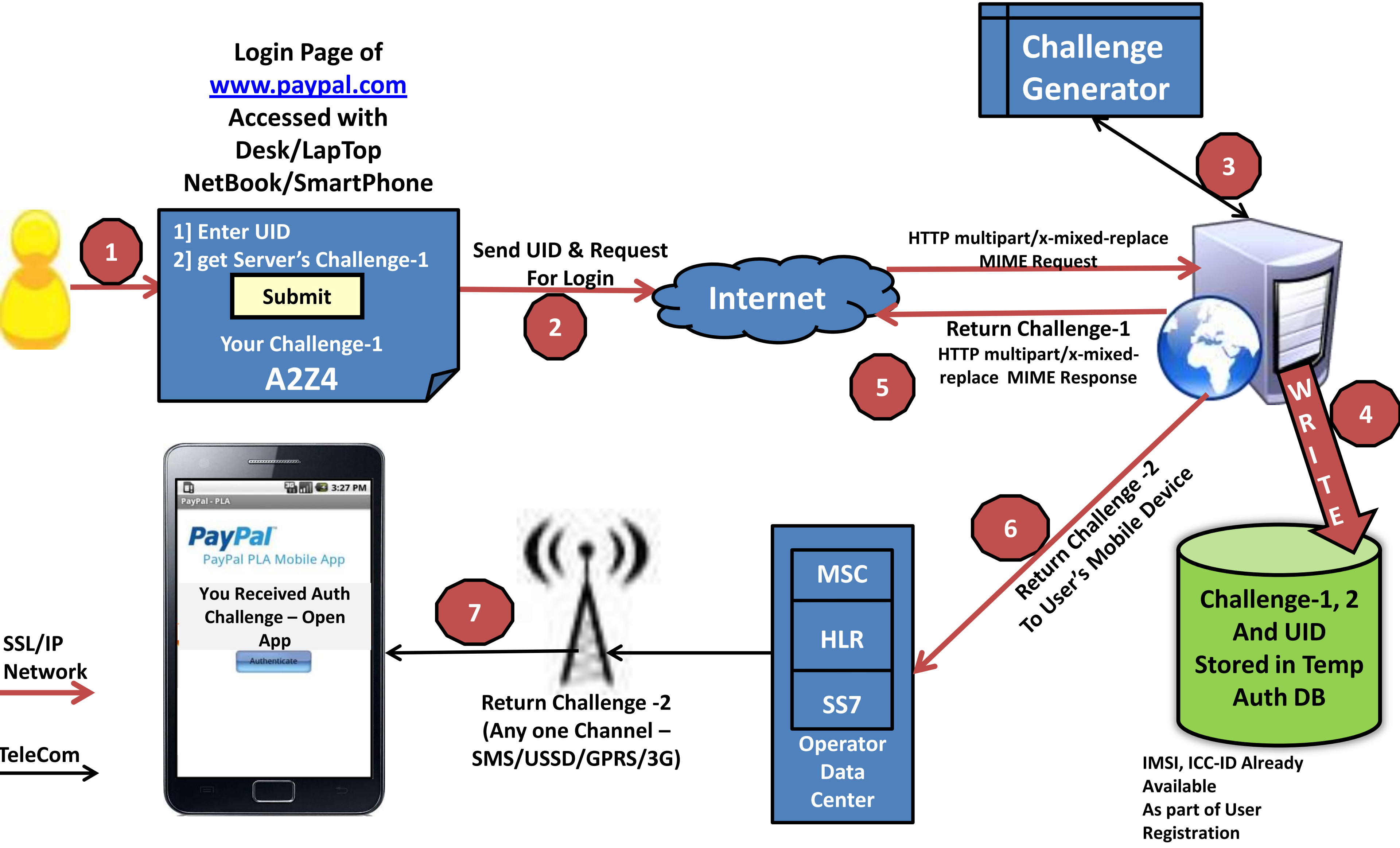
Step-6 Server reads the Push Response/SMS Message from User

Step-7 Server Decrypts Encrypted Packet with its Private Key

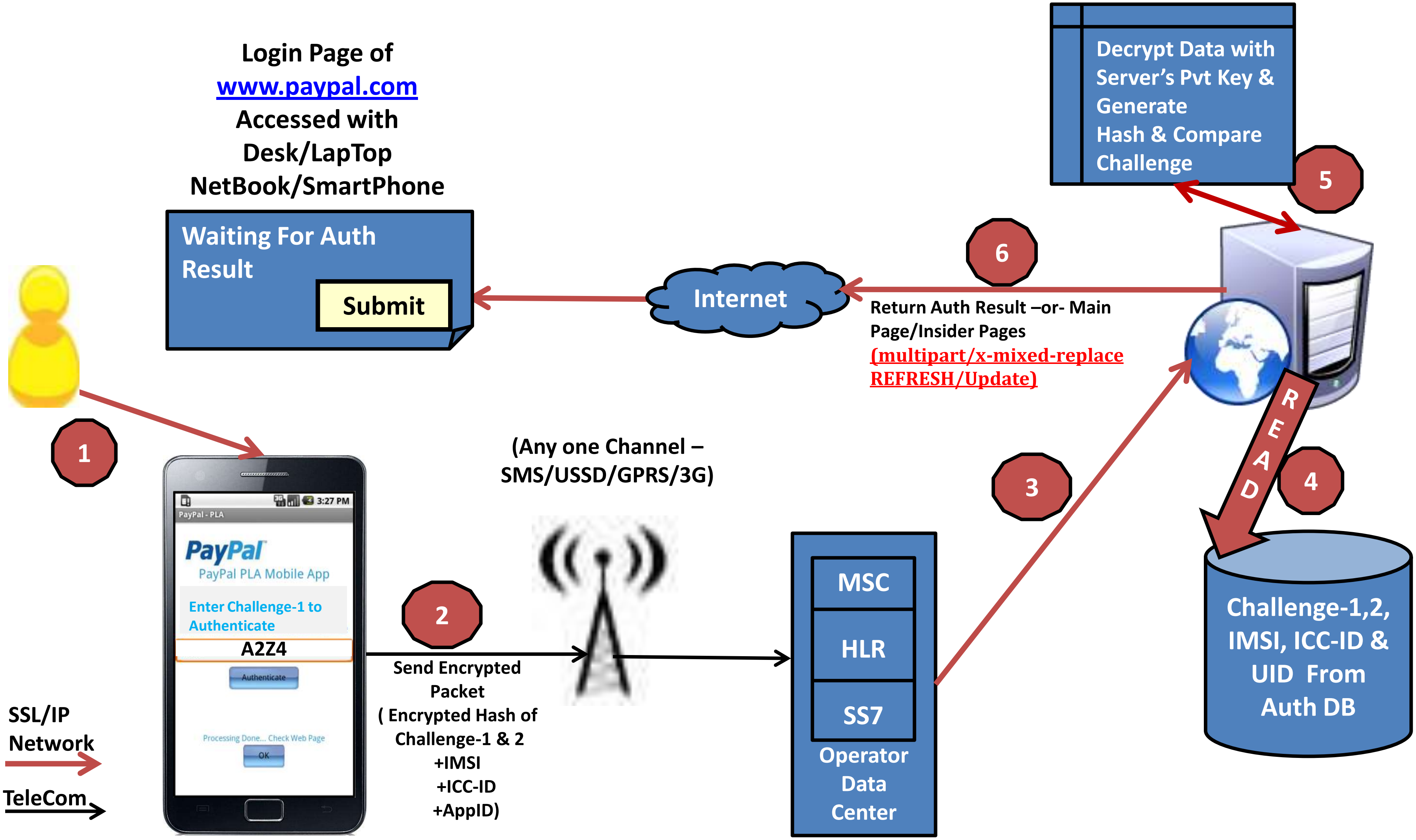
Step-8 Server loads ***C1+C2+IMSI+ICC-ID+AppID*** stored in the Database for that user's request and hashes again

Step-9 If Hashes Match then Welcome screen is pushed to the web user as a Response to ***multipart/x-mixed-replace***

Authentication Schematics



Authentication Schematics



Login Page of www.paypal.com Accessed with Desk/LapTop NetBook/SmartPhone

Waiting For Auth Result

Submit

Internet

Return Auth Result –or- Main Page/Insider Pages (multipart/x-mixed-replace REFRESH/Update)

Decrypt Data with Server's Pvt Key & Generate Hash & Compare Challenge

PayPal - PLA

PayPal

PayPal PLA Mobile App

Enter Challenge-1 to Authenticate

A2Z4

Authenticate

Processing Done... Check Web Page

OK

Send Encrypted Packet (Encrypted Hash of Challenge-1 & 2 +IMSI +ICC-ID +AppID)

(Any one Channel – SMS/USSD/GPRS/3G)

MSC

HLR

SS7

Operator Data Center

Challenge-1,2, IMSI, ICC-ID & UID From Auth DB

SSL/IP Network

TeleCom

Best Channel – Real Experience for PLA

#	Connectivity Protocol / Bearer Channel	Dev Cost	OS Comp	Initial Testing Cost	Integration Cost (Between Operator & Servers)	Connection Speed	Connection Type	Location Dependency	User Experience (Server Response Speed)	Setup Costs (H/W & S/W)	End User Charges	OPS Cost	Support (user compliants)
1	**SMS**	LOW	Devices that has Java 1.4 or above	MEDIUM	LOWEST	LOW	Store & Forward	Yes - LOW	LOW	LOW	LOW	MEDIUM	HIGH
2	**GPRS**	MEDIUM	Devices that has Java 1.4 or above	LOW	LOW	MEDIUM	Packet Based	Yes - LOW	SUPER	LOW	MEDIUM	MEDIUM	MEDIUM
3	**3G**	HIGH	Devices that has Java 1.4 or above	HIGH	HIGH	HIGH	Conn--Oriented	Yes - HIGH	SUPERLATIVE	HIGH	HIGH	HIGH	HIGH
4	**USSD-USSR Over SMPP**	**LOW**	**Devices that has Java 1.4 or above**	**HIGH**	**HIGH**	**HIGH**	**Session based (between Handset & N/W)**	**Yes - HIGH**	**SUPERLATIVE**	**MEDIUM**	**NIL**	**LOW**	**MEDIUM**

Best Channel with Best User Experience

USSR-Unstructured Supplementary Service Request (Network Initiated Push for Application Start-Up)

Competitors to PLA

Browser ID
Solid Pass **(All or some products)**
Google PIN Check/Verification Code

PLA, Browser ID, Solid Pass & Google PIN Check all are based on "**Ownership**" based authentication model and hence they all can be directly compared for

1. Speed of Auth/Z
2. Ease of Use (UI, Registration)
3. Portability
4. Adaptation Flexibility & Scalability
5. Security Aspects

NOTE: **PLA** is **NOT** a Funded project like its competitors and hence its peripheral security aspects needs some work.

OTP & PLA - Differentiators

	OTPs	PLA
1	Multiple Tokens - for each "Secure Banking Service“ - ICICI, HDFC, CITI	No need to carry multiple tokens for each "Secure Banking Service"
2	Remember UIDs or User Nos	***No remembering of passwords*** for any "Secure Banking Service“ - ***Only remember the user ID***
3	Remembering respective passwords for each User IDs or User Numbers	Easy to add new "Public Key" for any "Secure Banking Service” in same mobile app.
4	Changing respective passwords for each User IDs or User Numbers in Credential life cycle	Application Logic shall take care of selecting which "Public Key" to use to encrypt Tokens for which "Secure Banking Service"
5	Dependent on Mobile Network ***(Mobile OTPs & PLA Both)***	Can be used for "Authorization“ as well (Requires additional development)
6	Cost for HelpDesk/Support Calls for Login Issues/Resets Token Issuance, Maintenance Token Support calls	**Secure Banking Service can *avoid* the COSTS of** Login issues on the IP Network Password Strength/Expiry/Losses/Resets ***Only Mobile App Updates is unavoidable cost*** HelpDesk/Service Desk Calls

References

[1] Identity Theft 9.8% (IC3-2010) - 3rd Most Internet Crime
http://ic3report.nw3c.org/docs/2010_IC3_Report_02_10_11_low_res.pdf

[2] PoneMon Report – 2011 - Cost of Cyber Crime Study
http://docs.media.bitpipe.com/io_10x/io_101711/item_452026/2011%202nd%20Annual%20Ponemon%20Cost%20of%20Cybercrime%20Study.pdf

[3] SMS Bank Tokens Vulnerable
http://www.zdnet.com.au/sms-bank-tokens-vulnerable-rsa-339308633.htm

[4] One Time Passwords are not Secure – Analysis
https://infosecisland.com/blogview/11813-One-Time-Passwords-are-Not-Secure-Enough.html
http://www.nowires.org/Papers-PDF/OTPanalysis.pdf

[5] RSA Secure-ID Hardware Token Hacked
http://technorati.com/technology/it/article/rsa-hackedtime-to-panic-for-corporate/

[6] US Chamber of Commerce – Proposing No Passwords, Only H/W or Smart Phone based Login
http://arstechnica.com/tech-policy/news/2011/04/with-passwords-broken-us-rolls-out-internet-identity-plan.ars

[7] Response time reasons & panic of users for their lost or stolen mobiles
http://www.zdnetasia.com/hardware-vulnerable-in-two-factor-authentication-39342580.htm

[8] Token Types, Costs, Comparisons & Current Implementors
http://www.zdnetasia.com/war-of-the-tokens-62037260.htm

[9] Miscellaneous
http://news.techworld.com/security/3258312/hackers-break-us-government-smart-card-security
http://blogs.gartner.com/avivah-litan/2010/12/15/2011-threats-and-trends/
http://www.bankinfosecurity.com/articles.php?art_id=1732
http://www.bankinfosecurity.com/articles.php?art_id=2728

QnA

Appendix

- POC Exploit/Failure Scenarios
- Differentiators – OTP & POC
- OTP Costs & Cons
- References

POC Exploit / Failure Scenarios

- **POC Exploit-1- Replay SMS attack**

  Attacker can replay i.e. Capture the signal & resend it within the time frame – attacker would only help the end user of the POC

- **POC Exploit-2- Sending Fake SMS**

  Attacker can send fake SMS on behalf the POC User – but cannot receive SMS on behalf of POC User – Courtesy "**Control Channel**" of Mobile Network, for a successful authentication the attacker must receive the initial Push/SMS Message

- **POC Exploit-3- A total Compromise**

  For Successful compromise attacker must know & have: User ID, Cell Phone No, IMSI, ICC-ID, Token-1 & 2, AppID and the "**Control Channel**" to receive Network Message

POC Exploit / Failure Scenarios

- ## POC Exploit-4- Lost/Stolen Mobiles

  Mobile Phone is a ***precious*** device hence the time taken for an owner to discover loss of Mobile is ***likely to be much shorter*** compared to loss of tokens, which is used only while making a banking transaction.

  ----**Jukka Riivari, CEO & President of Meridea**

Source:
http://www.zdnetasia.com/hardware-vulnerable-in-two-factor-authentication-39342580.htm

- ## POC Exploit-5- Zero Protection Scenario

  Attacker having overpowered the POC User & Mobile Subscriber, took control of Mobile device & the Desktop/Laptop/NetBook – this POC will completely fail

- ## POC Failure Scenario–1- Multiple Users

  POC cannot be used in Least Developed Countries, where Micro-Payments are rampant for Multiple Users per mobile

OTP Costs & Cons

Hardware token

–Source -http://www.zdnetasia.com/war-of-the-tokens-62037260.htm

Banks	ABN Amro, China Construction Bank, Citibank Singapore, DBS, HSBC, OCBC, UBS, UOB
Pros	- Has been around longer - Not dependent on the mobile phone operator network - Does not require any downloads or setup
Cons	**-Inconvenience due to *"necklace syndrome",*** **-where customers with multiple Bank A/c with different Banks will have to carry multiple tokens** **-Higher implementation costs.** **-Experts estimate hardware's recurring costs to be around S$40 (US$24.50) to S$60 (US$36.74) per user per year, compared to under S$10 (US$6.12) per user per year for software-based tokens** **- Customer has to pay a replacement fee if it's lost** **- Not tamper-proof**

OTP Costs & Cons

Software token for mobile – Source- http://www.zdnetasia.com/war-of-the-tokens-62037260.htm	
Banks	**OCBC Singapore**
Pros	- Mobile phone is ubiquitous - No replacement fee; customer simply has to download the software application to his new phone
Cons	**-Dependent on the mobile operator network** **- Mobile phone can be as easily lost as hardware token, although chances of someone realizing his phone is missing are higher than it would be with the hardware token** **- Still very new & customers are less familiar with process, compared to SMS**

OTP Costs & Cons

SMS Tokens

– Source - http://www.zdnetasia.com/war-of-the-tokens-62037260.htm

Banks	**Citibank Singapore & Hong Kong, OCBC, Standard Chartered, UOB**
Pros	- Mobile phone is ubiquitous - People in Asia are familiar with SMS - Requires no training
Cons	**-Dependent on the mobile operator network** **- Potential issues like lost transmission and unexpected delay during festive seasons or when one is overseas** **- Mobile phone can be as easily lost as hardware token, although the chances of someone realizing his phone is missing are higher than it would be with the hardware token**