

# SASSO: Personal Identity Provider on Mobile Phone

NTT

Information Sharing Platform  
Laboratories

Kenji Takahashi

Copyright(c)2007 NTT Corporation. All  
Rights Reserved.

# What is SASSO?

- SASSO stands for Strong Authentication for Single Sign On
- SASSO means “pebble” in Italian
- SASSO is written as 颯爽 in Japanese, meaning “gallant, dashing, smart, jaunty”
- SASSO represents one’s identity

# Market trends in Japan

- Advanced mobile services have been deployed and widely accepted
  - Broadband – 3G available nationwide, HSDPA (up to 3.6 Mbps), ...
  - Built-in security – PKI, biometrics, NFC, ...
  - Advanced applications – payment, search, SNS, DTV...
  - From voice to data
  - Flat rate
- Also fixed broadband services have been pushed down
  - ADSL 40.6%, FTTH 28.2%
  - NGN will be available soon
- Identity management is an integral part of the future converged world
  - Advanced personalized data services to play the bigger roles
  - Subscription as a basis of identity
  - Subscription as a basis for one-stop service offering

# Problems: Strong authentication needed everywhere

- Passwords are often said to be insecure, but are still used everywhere
- Strong authentication has been proposed but not used as widely as desired because...
  - It may require the acquisition and installation of new hardware and/or software
  - People forget (or hate) carrying it
  - It may not be compatible with PCs that users want to use

# The Emperor's New Security Indicators

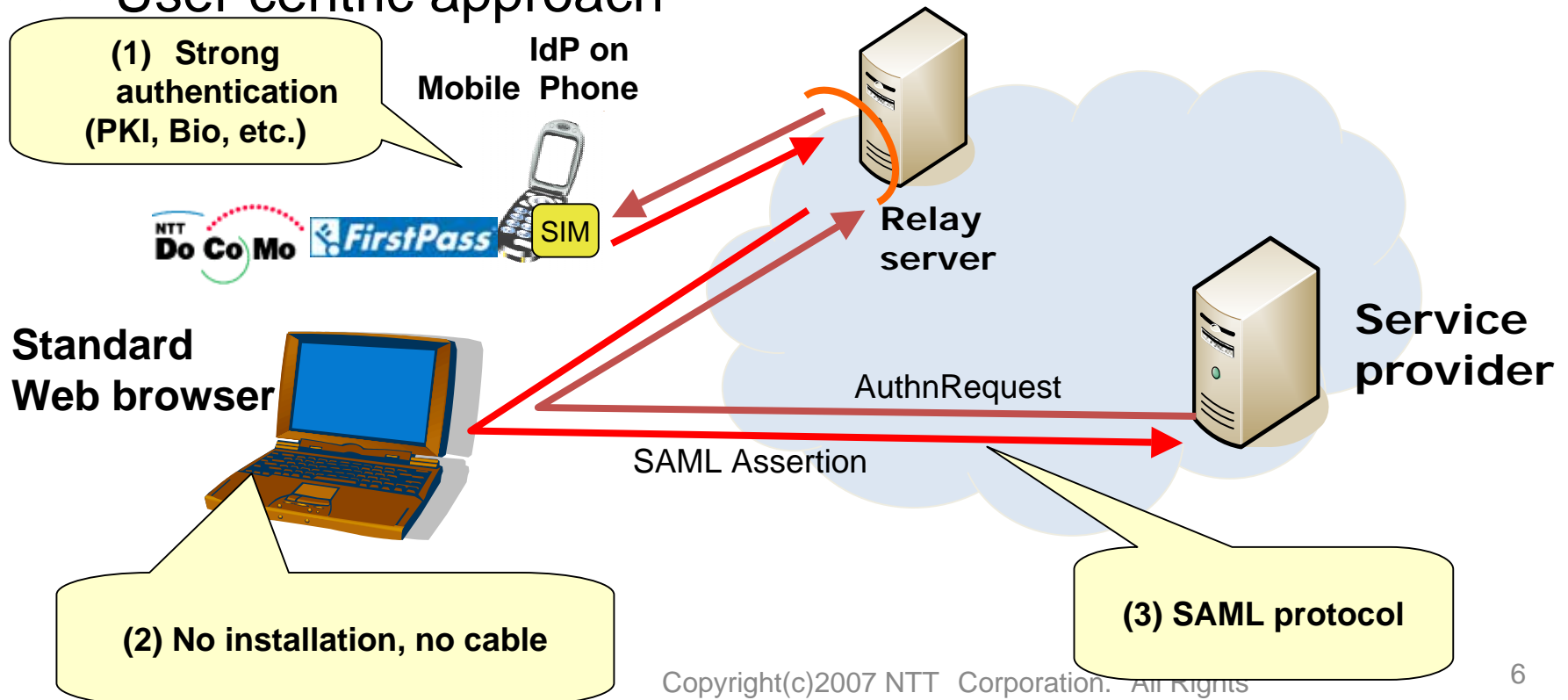
A study of online banking customers reveals that they entered their passwords even if:

- HTTPS indicators were missing  
=> 100%
- “Site authentication” images were missing  
=> 92 %
- A security warning page was presented  
=> 53%

S. Schechter et al., “The Emperor's New Security Indicators,”  
Proceedings of IEEE Symposium on Security and Privacy, 2007

# Solution: SASSO

- Enable single sign on to a PC with the strong authentication capabilities of a mobile phone
  - e.g. NTT DoCoMo's FirstPass, an authentication service
- No installation or cable or footprint on PC
- Standards-based approach avoids incompatibility
- User centric approach



# Slide show demonstration

# Login Page

Click

Net Life Garage - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

Net Life Garage

Net Life Garage Circle of Trust

What's single sign-on Need user account?

Categories

- Technologies
- Jobs
- Yellow Pages
- Map
- Weather
- Shopping
- Entertainment
- Life
- Travel

NLG Tools

- Mail
- Address Book
- Calendar
- Blog

Sign-On

Get New Account  
Create New Account

Circle of Trust Members

- Shopping
  - Fruits Catering
  - Chamonix
  - HOROYO!SUSHI Deliveries
  - OFFROAD
  - avetaxi
  - polochestno
  - SAKABA BOSSY
- Entertainment
  - Hobby Club
  - DVD Drive DVD Rental
- Money and Banking
  - MIRAI BANK
  - CHIKUZO Securities
- Health and Medical Care
  - Hinomaru Cosmetic Store
  - Drug Space
- Community
  - TAKIBI .NET

Today's News

- [U.S. considers options to Election Day delay](#)
- [Rocket problem delays satellite launch](#)

NET LIFE GARAGE Special

- [NTT DoCoMo: i-mode users outside Japan exceed 3 million](#)
- [NTT Com launches global voice/video unified solution](#)

Recommendations

- [Liberty Alliance Project: Defining identity for global business](#)
- [NTT Group press release](#)
- [Do you know Japanese mayonnaise pizza?](#)
- [e-Authentication Portal](#)

NLG COT This site provides authentication service for Net Life Garage trust of circle.  
[Click here for more information](#)

NTT  
Powered by NTT

Copyright (C) 2004 Net Life Garage All Rights Reserved.

完了



# Login Page

Net Life Garage - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

Net Life Garage

Net Life Garage Circle of Trust

What's single sign-on Need user account?

Categories

- World
- Technologies
- Jobs
- Yellow
- Map
- Weather
- Shopping
- Entertainment
- Life
- Travel

Sign-On

Get New Account or Create New Account

Circle of Trust Members

- Shopping
- Community

NTT

Powered by NTT

Copyright (C) 2004 Net Life Garage All Rights Reserved.

完了

Please enter your Mobile Phone IdP's URL.

https://

OK キャンセル

# Launch IdP application



# Login Page

Net Life Garage - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

Net Life Garage

Net Life Garage Circle of Trust

What's single sign-on Need user account?

Categories

- World
- Technologies
- Jobs
- Yellow
- Map
- Weather
- Shopping
- Entertainment
- Life
- Travel

Sign-On

Get New Account or Create New Account

Circle of Trust Members

- Shopping
- Community

Please enter your Mobile Phone IdP's URL.

<https://mobile-idp.ntt.jp/abe/>

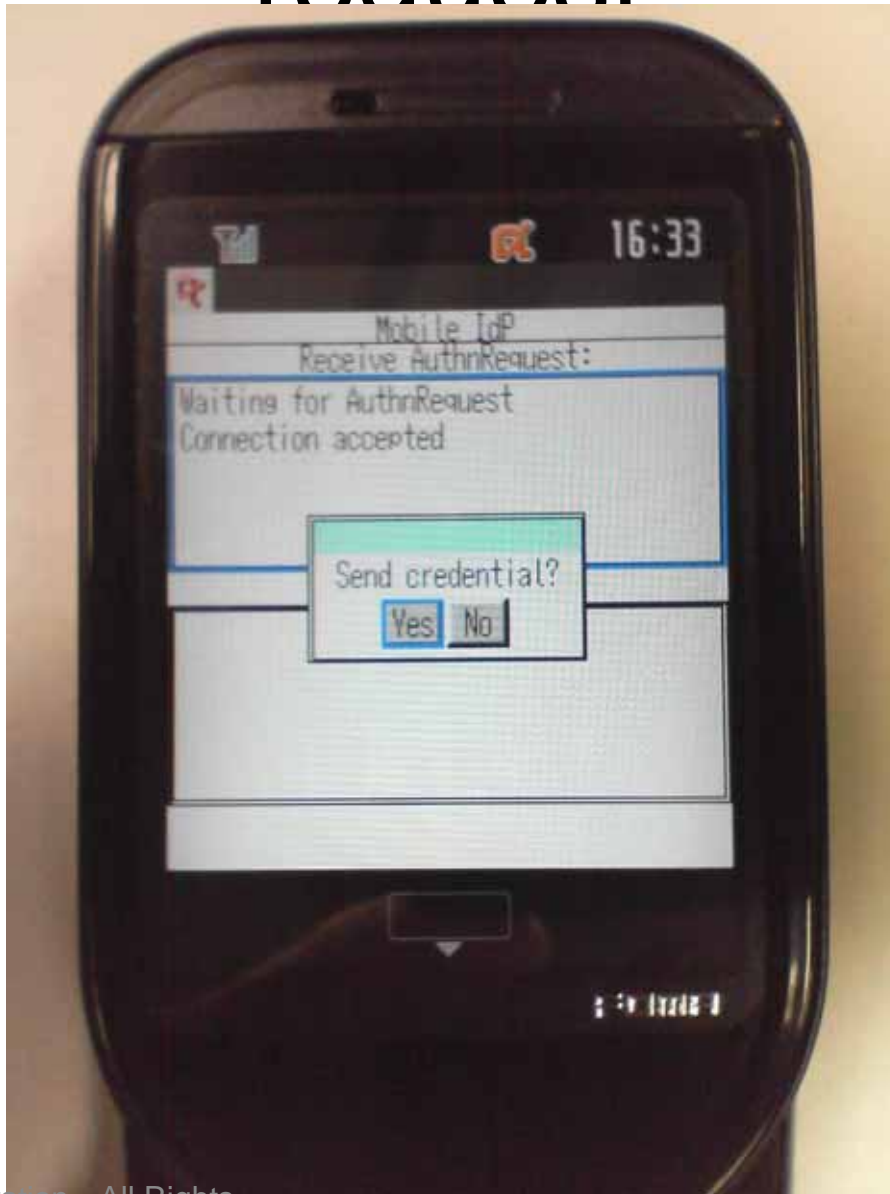
OK キャンセル

NTT  
Powered by NTT

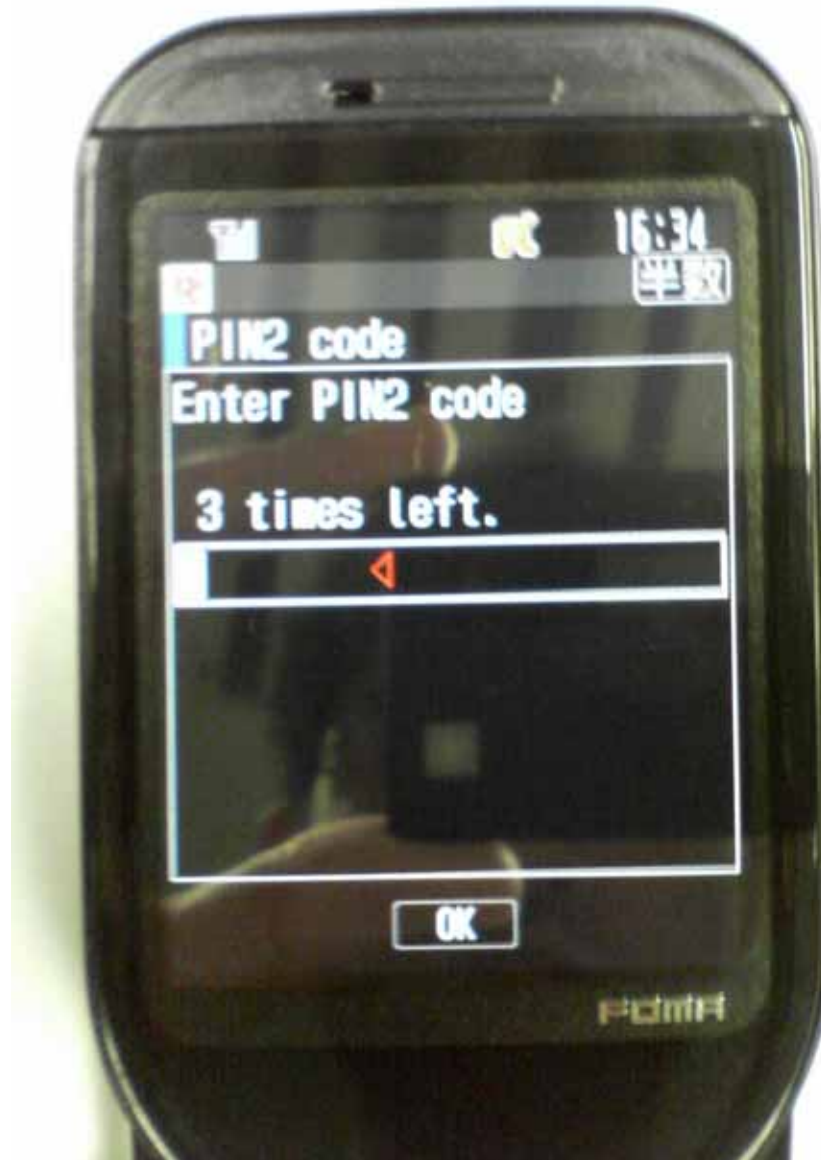
Copyright (C) 2004 Net Life Garage All Rights Reserved.

完了

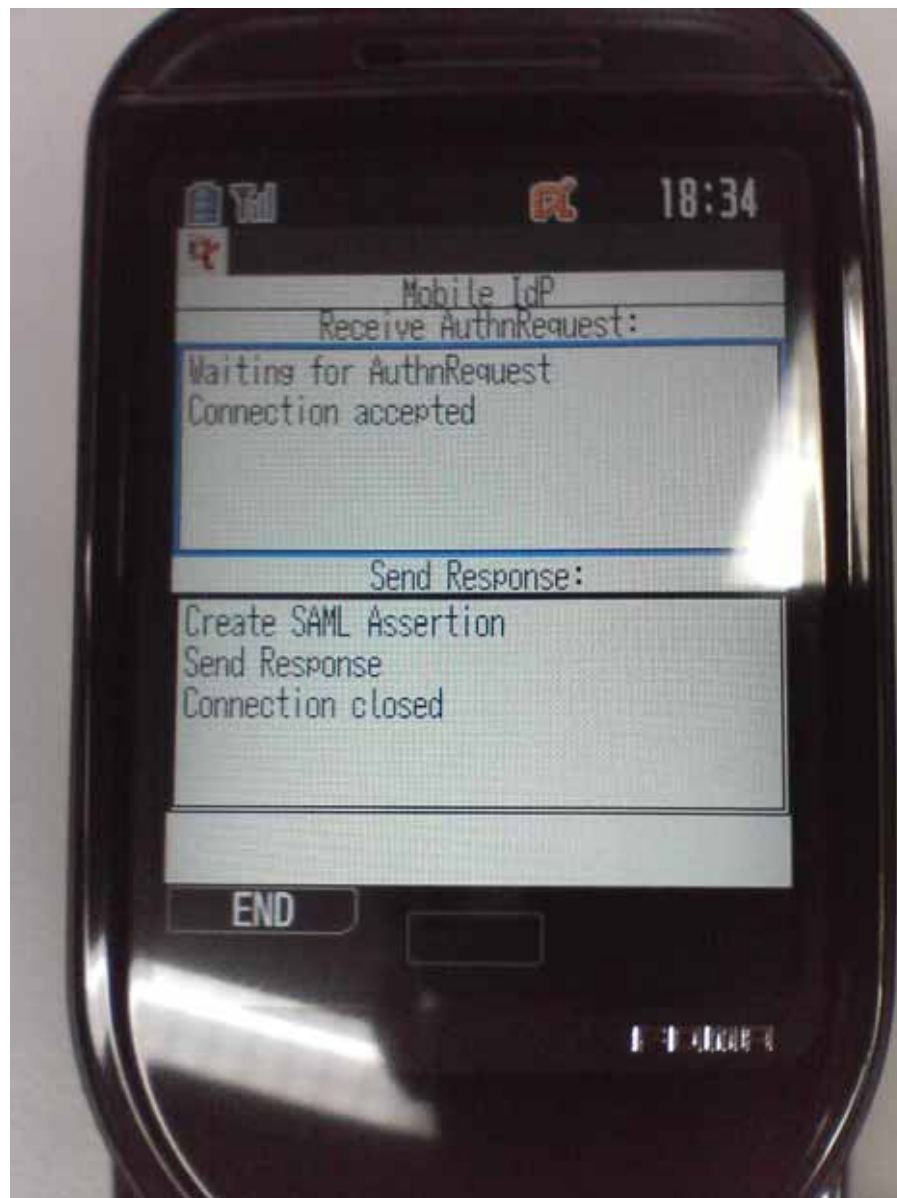
# Notification of authentication request



# PIN code authentication



# Send SAML assertion



# Welcome page

Net Life Garage - Mozilla Firefox

ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

Net Life Garage

Username: Tsuyoshi Abe

Net Life Garage Circle of Trust

What's single sign-on Change your profiles Detail settings Contact us [Directly sign-on to other providers](#)

**Categories**

- World
- Technologies
- Jobs
- Yellow Pages
- Map
- Weather
- Shopping
- Entertainment
- Life
- Travel

**Single Logout from Circle of Trust** **Logout from this site**

Hi Tsuyoshi Abe,  
Thank you for visiting Net Life Garage Portal

- Tsuyoshi Abe has been authenticated by Net Life Garage Circle of Trust.

**NLG COT** This site provides authentication service for Net Life Garage trust of circle.  
[Click here for more information](#)

**Circle of Trust Members**

- Shopping
  - Fruits Catering
  - Kobe House Chamonix
  - HORO'SUSHI Delivers
  - Tavetaivala
  - Yodoko
  - SAWABA Bogyu
  - OSAKA
- Entertainment
  - Hobby Club
  - DVD Online DVD Rental
- Money and Banking
  - MIRAI BANK
  - CHIKUZO Securities
- Health and Medical Care
  - Hinomaru Cosmetic Store
  - Drug Space
- Community
  - TAKIBI .NET

Powered by NTT

Copyright (C) 2004 Net Life Garage All Rights Reserved.

完了

Slide show demonstration

[Sequence flow](#)

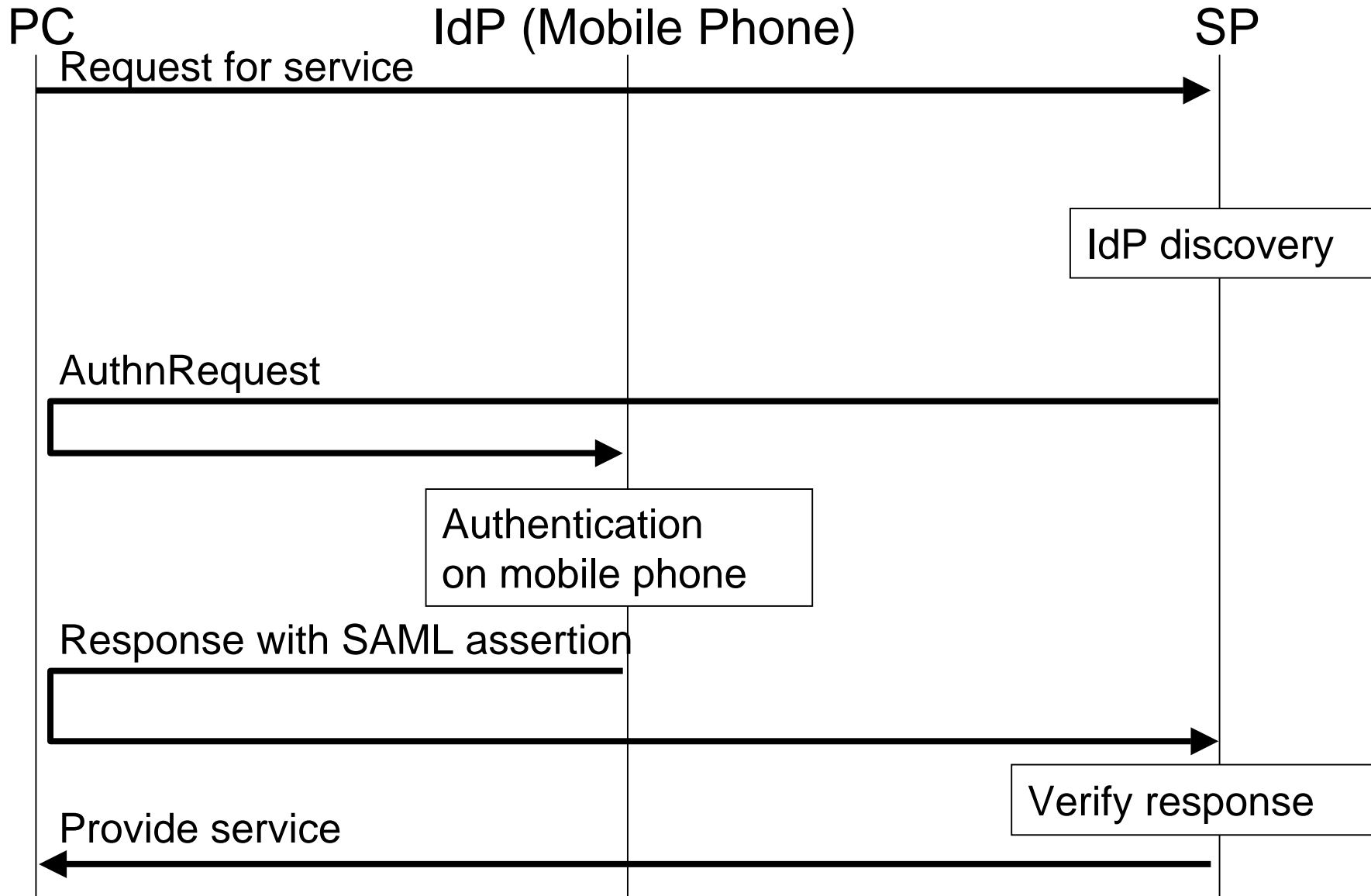
Relay Server

Performance

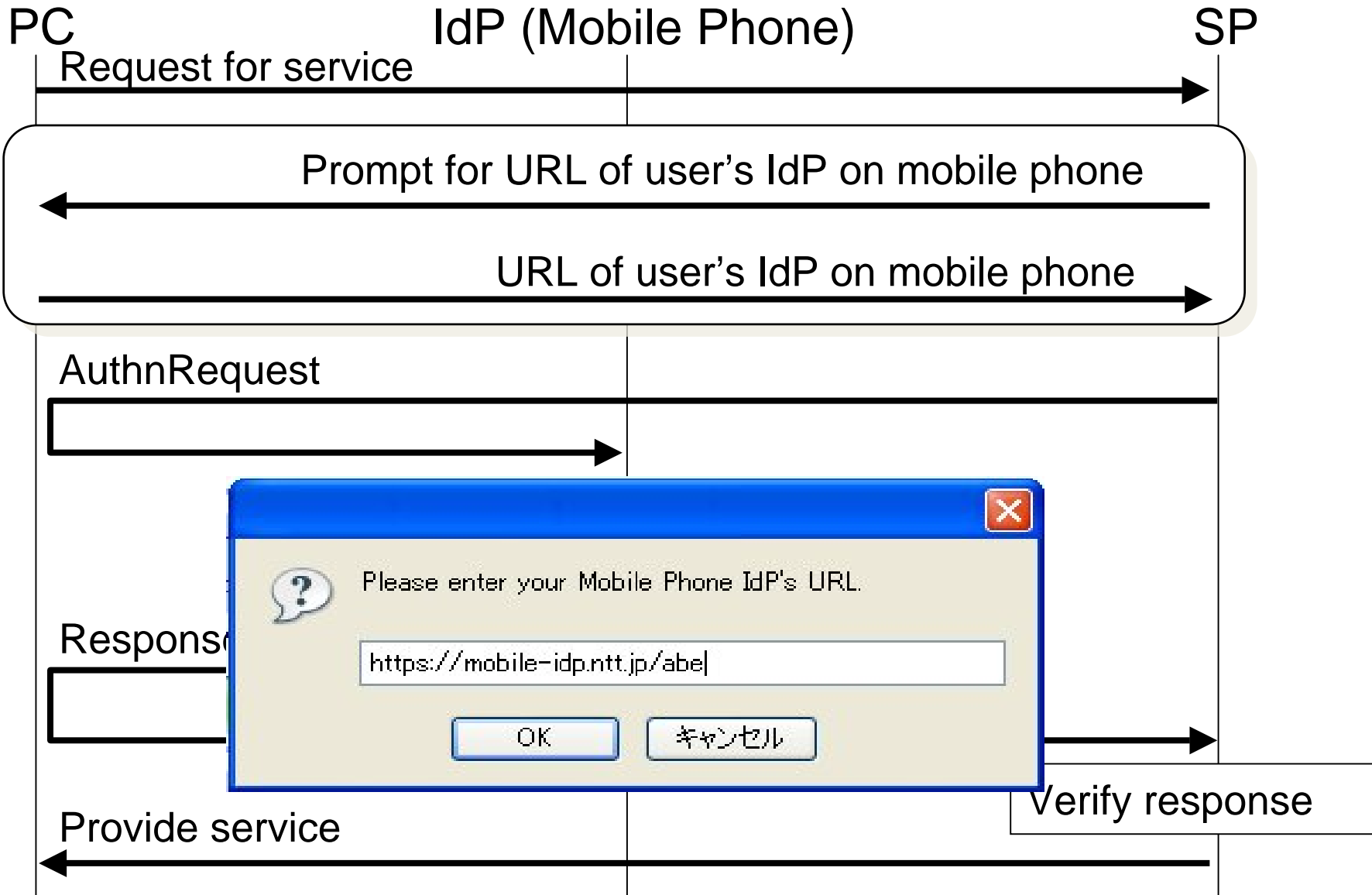
# Sequence flow



# Typical sequence flow



# IdP Discovery



Slide show demonstration

Sequence flow

[Relay Server](#)

Performance

# Relay Server

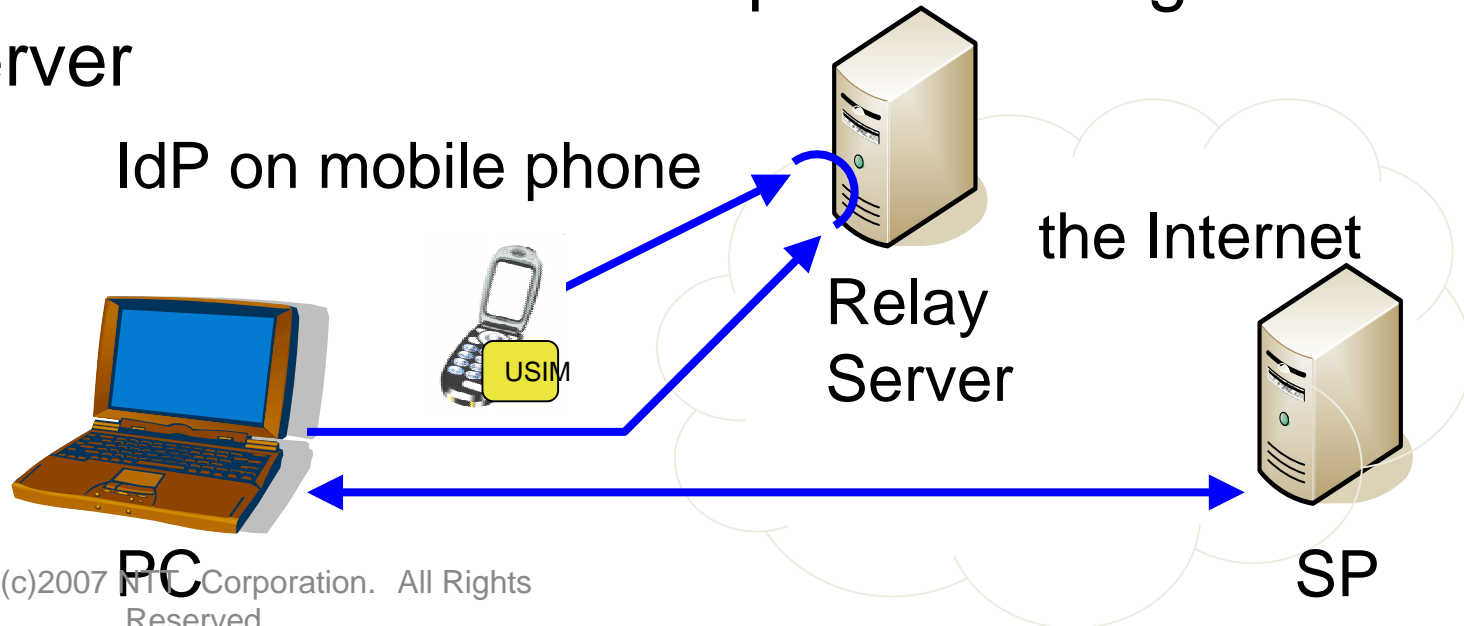
# Enabling Mobile Phones to act as Servers

## Problem

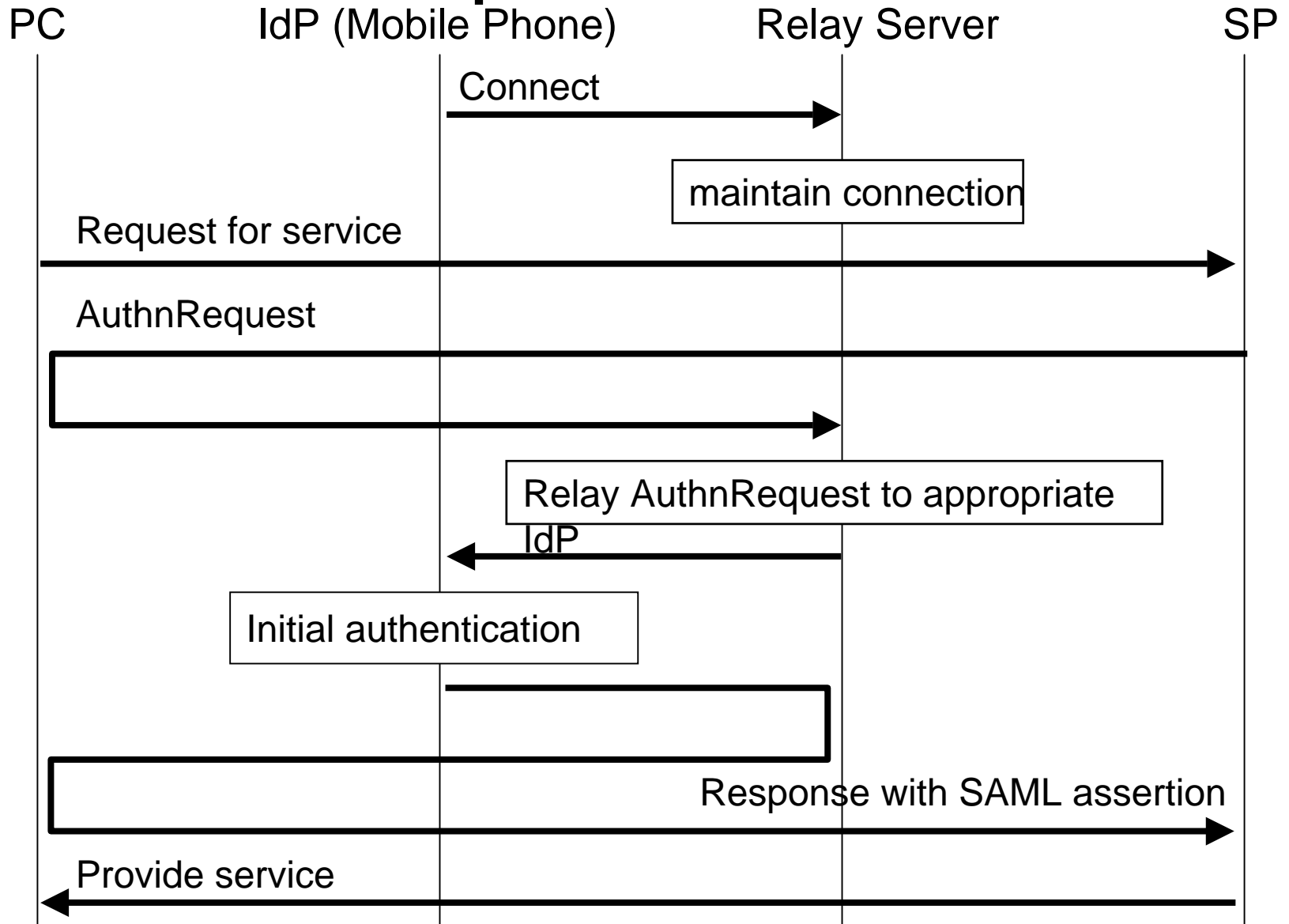
- PC cannot access mobile phone by HTTPS directly

## Solution

- Mobile phone accesses the relay server
- Relay server maintains the connection
- PC accesses the mobile phone through the relay server



# Sequence Flow



# IdP URL

## Statically allocated IdP URL

**https://mobile-idp.ntt.jp/abe**

**https://mobile-idp.ntt.jp/itoh**

Common part  
(relay server URL)

Distinct part  
(e.g. username)

## Dynamically allocated IdP URL

**https://mobile-idp.ntt.jp/14ety38r**

Common part  
(relay server URL)

Distinct part  
(random string)

Slide show demonstration

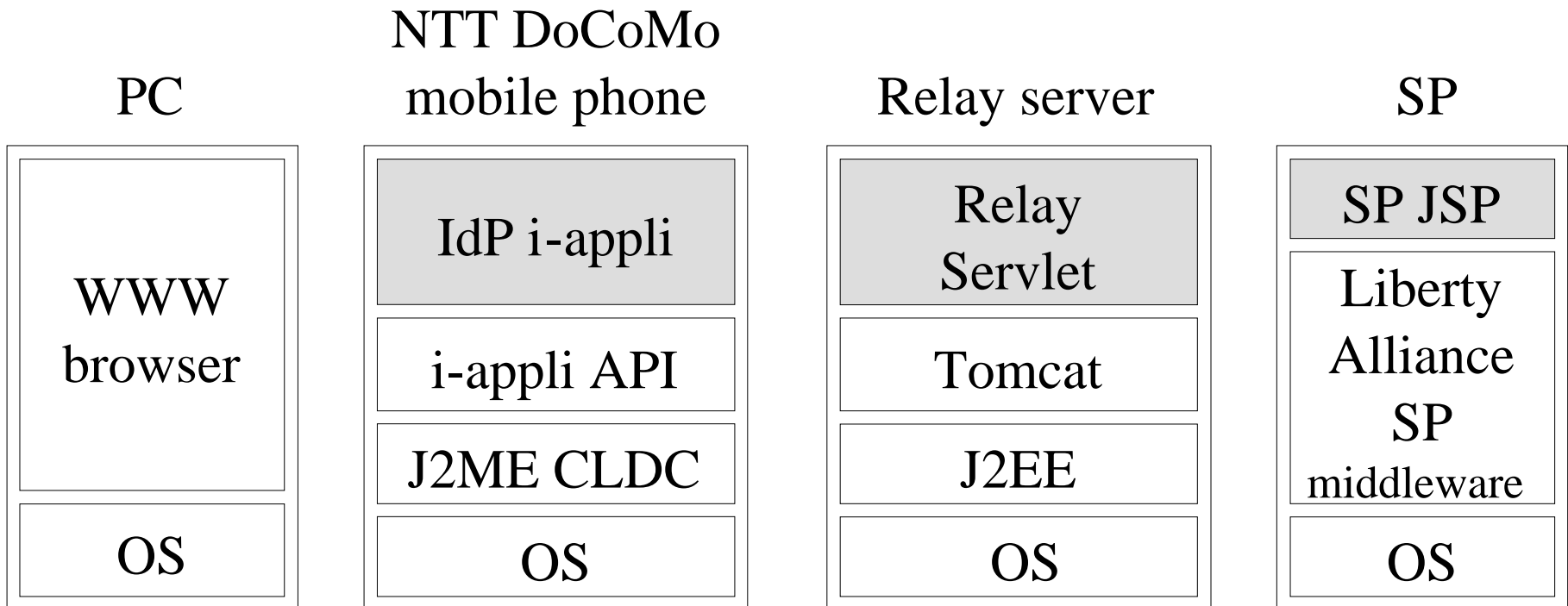
Sequence flow

Relay Server

Performance

# Performance

# Prototype System Configuration



Legend:

Newly developed component for SASSO

Conventional component



# Performance

## Specifications of mobile phone

Model	NTT DoCoMo F903i
CPU	SH-Mobile G1
Communication speed	384 kbps

## Processing time of IdP on mobile phone

Process	Time [seconds]
Communication	3
Digital signing	3
Other	0.4

# Future

- Mobile attribute provider capability
- Multi-protocol interoperability
  - OpenID, CardSpace, etc...
- Home identity center for net-connected appliances
- Adoption for VRM (Vendor Relationship Management)