Mobile Connect Accelerator
An HPE Digital Persona solution
Building a modern client relationship
With customers Digital Persona

Who is your customer
Know your customers to provide services they value

What services do they value?
Move away from volume based plans

When and where are they?
Reach out at the right context and most convenient situations

Why they are happy (or unhappy)?
Put the data together for a complete picture of your subscribers

Is their online presence secure and protected?
HPE Digital Persona

Securing and enabling a user friendly, flexible digital presence

Charging and rules engines
- PCRF
- OCS
- Service mediation

Retention
- Revenue assurance
- Subscription fraud

Retention
- Real-time analytics
- Complex event processing

Universal Identity Repository (UIR)

Digital Persona Solutions
- Device Entitlement
- Mobile Connect
- Single Sign-on
- Intelligent Messaging
- Subscription Manager

Core
- EIR
- AAA
- HLR/HSS
- DRA
HPE Mobile Connect
Enabling operator-based authentication and identity federation

Multiple disparate accounts

Service providers

Data breach

Personal profiles & critical data

Unverified identity
Identity theft

Basic profile

Client apps

Strong SSO

SIM-based authorization

HPE Identity Gateway

Microsoft

Facebook

Google+

Twitter

HPE Identity Gateway

SSO

Service providers
HPE Mobile Connect Solution
Brings Operators and Mobile Phones to the forefront of the Authentication Procedure for Service Providers

1. User clicks on a “Mobile Connect” button to access a service.
2. Service Provider requests authenticating Operator from the Discovery function (API Exchange).
3. Service Provider makes a request for authentication using OpenID with Mobile Connect profile.
4. Operator selects appropriate authenticator depending on request for assurance and capabilities.

Mobile Connect enabled apps

Users with SIM-based devices

Service providers

Operator service network

HPE Identity Gateway

Discovery provider

API exchange

1. User clicks on a “Mobile Connect” button to access a service.
2. Service Provider requests authenticating Operator from the Discovery function (API Exchange).
3. Service Provider makes a request for authentication using OpenID with Mobile Connect profile.
4. Operator selects appropriate authenticator depending on request for assurance and capabilities.
HPE Mobile Connect Solution Components
On Premises solution

- HPE Mobile Connect SSO
- Access manager and load balancer
- Identity manager
- Rules engine
- Notification server
- Provisioning manager (optional)
- Profile data manager (optional)

Connection Points:
- LDAP/ SOAP/ JDBC
- SMPP
- USSD
- JSON
- JMX
- JDBC
- SFTP

Other Components:
- Reports
- OA&M GUI
- Administrators
- Analytics (optional)

Supports:
- Sub DB
- SMS
- USSD
- OpCo SMSC
- OpCo USSD GW
HPE Mobile Connect Solution Architecture
MCX Compliant Hosted Solution Options

HPE SSO Platform
Front end
Access Manager and Load Balancer

Back end
Identity Manager and Authenticators

Service provider apps

Hosted at HPE Cloud

SMS ➔ USSD ➔ Sub DB
LoA 1-2

LoA 3-5

HPE SSO Platform
Front end
Access manager and load balancer

Back end – OpCo N
Identity Manager and Authenticators

Service provider apps

Hosted at HPE Cloud

SMS ➔ USSD ➔ Sub DB
LoA 1-2

LoA 3-5
Thank you