



# Valimo Mobile Identity Platform for financial services

Solution brief



## The Valimo Mobile Identity Platform running on HP Integrity NonStop servers sets the security standard in the financial services industry.

In the increasingly complex world of global banking, financial institutions face myriad challenges. The most pressing one is security: Banks must deal with fraud attempts that are becoming more sophisticated by the day. Other challenges include cost reduction, customer churn, and customer convenience.

Valimo Wireless offers a unique portfolio of security and mobile identity solutions—the Valimo Mobile Identity Platform—to address these challenges. By enabling a secure communication and transaction environment, these easy-to-use solutions enable a host of value-added services (e.g., payments, Internet banking, voting, or gaming) and promote consumer loyalty. Valimo solutions support different subscriber identity module (SIM) card types and work with any GSM phone on the market.

The preferred platform for Valimo security and mobile identity solutions is the HP Integrity NonStop server, based on the industry-standard Intel® Itanium® 2 processor. The Integrity NonStop server delivers superior performance, unrivaled availability, virtually unlimited scalability, and failsafe data integrity—all at the lowest total cost of ownership (TCO) in the industry for enterprise-class computing systems.

## How it works

Online banking provides a useful example. If you use an Internet bank, you need to do two things: You need to log in, and you need to confirm transactions once you have logged in. Many security schemas have been developed to accomplish these tasks. For example, the consumer may transmit both the login user identification (user ID) and password to the bank via a browser; this is generally considered the least secure approach. Banks can issue “scratch” cards with a list of one-time passwords, so that each code is used only once. This approach is more secure, but it is expensive for the bank and inconvenient for the consumer.

The bank might also provide a hardware “token” (a battery-operated keypad with a display) to generate one-time passwords. Using a token involves multiple steps: receiving a number from the bank, entering the number into the device, reading the password from the device, and, finally, typing the password into the browser. Again, this is an expensive and cumbersome process.

By contrast, the Valimo solution—which leverages advanced wireless PKI (WPKI) technology—provides simplified, convenient, cost-effective, and highly secure authentication and authorization for Internet banking. The consumer still communicates with the bank via a PC-based browser, but a digital signature generated in the mobile phone is used both to authenticate the user and to authorize transactions.

In this example, Valimo Validator – MSSP authenticates the user for the transaction; it receives the signed message, performs the signature verification process, looks for the certificates, validates them, and accepts or rejects the request for authentication. Valimo ID Server is integrated into the bank’s Internet banking solution. When the consumer sends a login transaction or initiates a payment transaction, the Internet bank calls the Valimo ID Server, which then calls the mobile phone.

Valimo ID Server can support other authentication methods as well, including one-time passwords; in that case, the Valimo ID Server would convey a one-time password to the mobile phone as a short message service (SMS) text.

The use of two separate communication channels—one for user authentication and transaction authorization, and the second for delivering the service (e.g., access to a bank account)—results in leading-edge security for online banking. This approach is also very cost-effective for the bank, because the consumer has already purchased the mobile phone. There is no need for the bank to pay for producing, distributing, and managing scratch cards or hardware tokens.

## Two-factor, two-channel security

Security is based on two things: something you have in your possession, and something you memorize. This “two-factor” security approach is applied broadly, from using a debit card at a POS terminal (card + PIN) to more sophisticated methods that secure online banking services.

The Valimo Mobile Identity Platform solution employs the mobile phone and a digital signing application on the SIM card to provide two-factor security, in addition to using separate communication channels to create a new dimension: two-factor, two-channel security. The solution is cost-effective for the bank and convenient for the consumer, and it supports different security schemas for outstanding flexibility and choice. Combined with the superior service level provided by the HP Integrity NonStop server, the Valimo Mobile Identity Platform solution sets the standard for security in financial services.

## HP Integrity NonStop server

The gatekeeper to the bank’s services is the most business-critical part of the e-business offering. It is the availability and performance of the HP Integrity NonStop server, hosting the Valimo software suite, that provides the responsiveness and excellent customer experience of the e-banking services.

The core components of the Valimo Mobile Identity Platform for financial services are Valimo Validator, Valimo ID Server, Valimo Messaging Server, and Valimo Registration Server. They all run on the Integrity NonStop server.

### **Valimo Validator – MSSP**

Valimo Validator – MSSP is a standard Mobile Signature Service Provider (MSSP) platform. It provides the core server-side functionality that a mobile operator needs in order to provide WPKI services. Valimo Validator – MSSP covers the entire signature transaction life cycle by managing signing requests, the signature verification and certificate validation process, and the transaction recording requirements.

### **Valimo ID Server**

Valimo ID Server is an Authentication, Authorization, and Accounting (AAA) server solution. It provides a secure way to define who may access a given resource—for example, an e-mail, file, or virtual private network (VPN) server—specifically what each individual may access, and when and how this access may occur. Valimo ID Server provides a range of authentication methods through various interfaces, including (but not limited to) WPKI. In addition, Valimo ID Server supports easy and flexible integration with existing user databases and other network infrastructure components.

### **Valimo Messaging Server**

Valimo Messaging Server provides a solution for managing messaging complexity. It can route messages between different messaging centers and services, generate statistics, and facilitate network management. It gives the message platform owner full business control over the mobile value chain, along with the flexibility to change the service portfolio. Valimo Messaging Server supports a variety of different message types, including SMS, Multimedia Messaging Service (MMS), Wireless Application Protocol (WAP) Push, Modular Storage System (MSS), and Simple Mail Transfer Protocol (SMTP). It also enables communications with a wide range of current and future mobile signature creation devices (MSCDs), allowing mobile operators to simplify their infrastructure.

### **Valimo Registration Server**

Valimo Registration Server provides mechanisms for WPKI user information management, making it possible to manage end-user credentials throughout their life cycle. It can be deployed by either a certification authority (CA)—for example, a mobile operator or a corporation—or a bank. Valimo Registration Server can be customized to suit many common registration models that identify the end user.

## For more information

To find out more about the Valimo Mobile Identity Platform solution, visit [www.valimo.com](http://www.valimo.com).

For more information on the HP Integrity NonStop server, visit [www.hp.com/go/integritynonstop](http://www.hp.com/go/integritynonstop).

## HP Services

HP's end-to-end Service Solutions built on the Solution Lifecycle (SLC) process, offers consistent quality and service levels for the Integrity NonStop servers. The SLC process helps achieve rapid productivity and maximum availability by examining specific needs at each of five distinct phases (Plan, Design, Integrate, Install, and Manage) and then designing solutions around those needs. We offer three different Service Solutions designed to meet customer needs. They are:

### HP Critical Service Solution

- Startup and Deployment Services—build the solution to your exact specifications, complete the installation, and make the solution application-ready.
  - Assessment and Design services—define requirements and translate your business and technical needs into a solution that melds the necessary hardware and software
  - Deployment Management—upfront project coordination from HP
  - Education Services—training curriculums relevant to needs and existing expertise based upon a needs analysis
- HP Critical Service—comprehensive ongoing support designed to help minimize the business impact of downtime for mission-critical applications

### HP Proactive Service Solution

- Startup and Deployment Services
- HP Proactive 24 Service—integrated hardware and software support, including proactive and reactive services to improve stability and availability across your IT environment

### HP Foundation Service Solution

- Startup and Deployment Services
- HP Support Plus 24 Service—integrated hardware and software support services designed specifically for your technology.

For more information: [www.hp.com/services/nonstop](http://www.hp.com/services/nonstop).

To learn more, visit [www.hp.com/go/integritynonstop](http://www.hp.com/go/integritynonstop)

© Copyright 2006 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA0-9344ENW, December 2006

