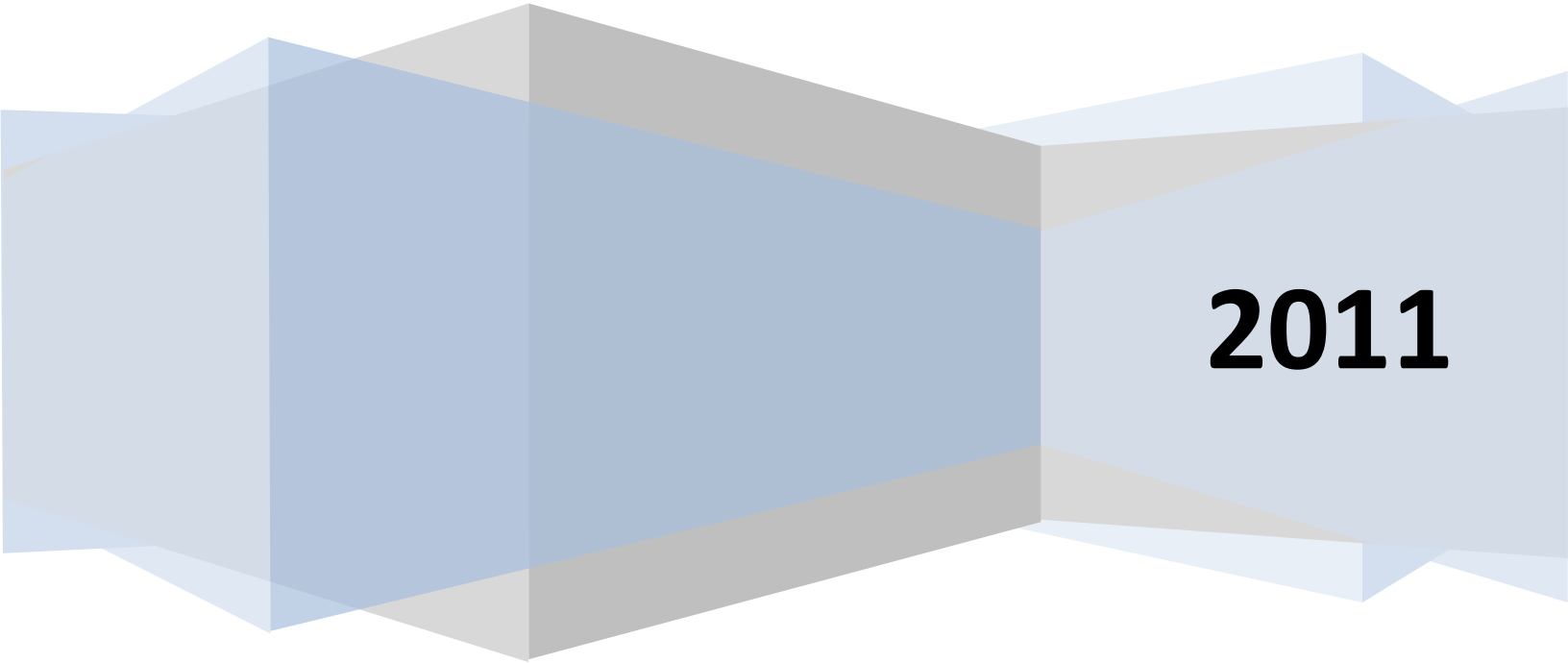
Implementation of One-Time Password (OTP)

Two-Factor Authentication System from ViSolve for Banks

ViSolve Marketing Team



2011

ONE-TIME PASSWORD SYSTEM

As Banks strive to enhance their Customer-Touch-Point scenarios by the introduction of new innovative services & capabilities including Net-Banking to facilitate basic enquires, money transfers and simple payment transactions. Banks have been experiencing the Web-enabled operations has had tremendous acceptance from the Customers with exponential growth. Banks in order to maintain competitive advantage coupled with a commensurate increase in the number and sophistication of online services are leveraging on their IT infrastructure.

Computer security has been the victim of the "year of the…" syndrome with firewalls, intrusion detections, VPNs, and now Certification Authorities (CAs) for Public Key Infrastructure (PKI). One form of attack on web-based platforms is phishing and eavesdropping on network connections to obtain authentication such as Login IDs and Passwords of legitimate users. Given enough time for attempts, it's relatively easy for unauthorized intruders to crack a static password. With Cyber-Crime on the rise enterprise IT administrators are finding ways out, to introduce improved levels of authentication to gain customers trust.

Setting up Public Key Infrastructure (PKI) with CA – Certificate authorities and managing it could prove to be a costly affair, with year-on-year recurring investments. Introducing Visolve's HP-UX AAA Solution: One-Time-Password (OTP) with Two-Factor Authentication system, your organization can easily provide users a secured platform to have access to data 24X7 and for any online transactions. The OTP system protects against external passive attacks against the authentication subsystem. The OTP authentication system allows you to cost-effectively implement strong authentication in any RADIUS-enabled gateway including VPN solutions and web access solutions.

A simple static password solution can become a liability on the Banks for online transactions. Unlike static passwords, a one-time password changes each time user logs in with the password being generated either by time-synchronized or counter-synchronized methods that typically requires the user to carry a small piece of hardware in his key-chain.

ONE-TIME PASSWORD SYSTEM

SOLUTION METHODOLOGY

Visolve's HP-UX AAA Server and OATH: Standards based Two-Factor Authentication offers:

1) Authentication using two independent methods typically something you have (device) and something you know (password)

2) One-Time Password (OTP)

2. a) Password only valid for single use

- Two-Party model: Client and Server utilize OTP software or hardware to generate and validate password.
- Two-Channel model: High value transactions can be authenticated by an OTP being delivered via secondary mechanism, (e.g., email, voice, SMS)

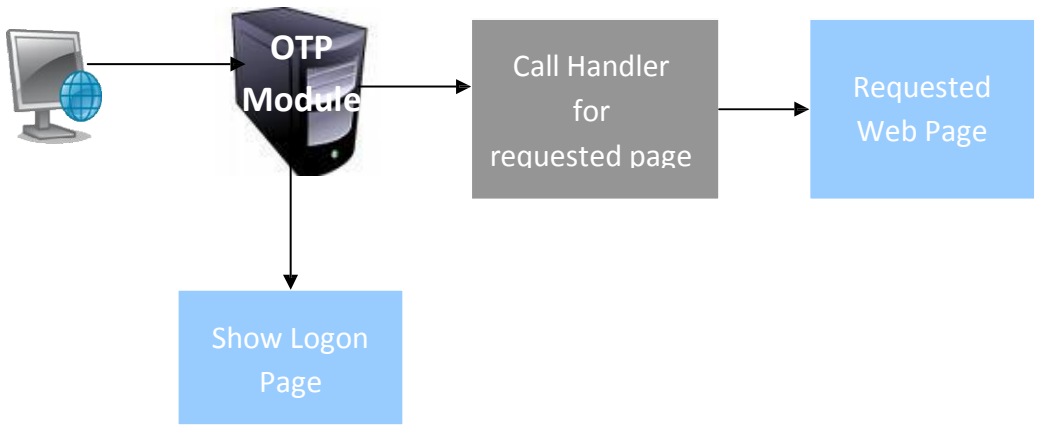
2. b) OATH

- Open Standard for OTP generation (http://openauthentication.org) Sequence based algorithms, built on shared secret
- Supported by nearly all of the token device vendors

ADVANTAGES OF OATH V/S PROPRIETARY OTP

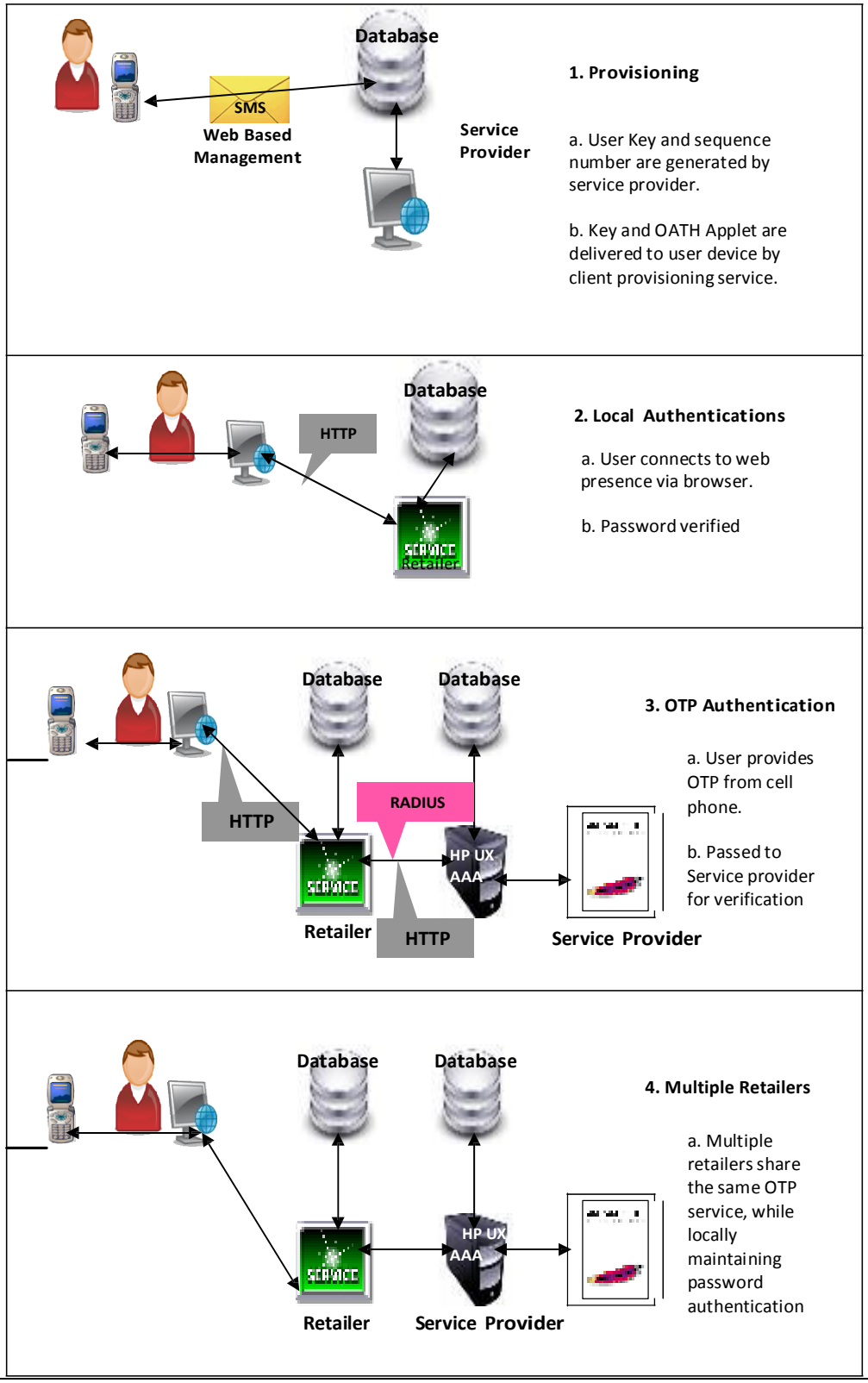
Cost Effectiveness:

- Concept of Sequence based algorithm allows for low manufacturing cost of token devices
- Multiple User deployment scenarios
- Standalone token device
- Built into consumer electronic components like memory cards
- Software for Cell phone applets or hardware/software (e.g. TCG)
- Multiple delivery-channel solutions like SMS
- Independent components like Client, Server and user management components can be purchased separately
- Ease of availability of tokens in open market at competitive rates
- Multiple application support with single Authentication Server
- No royalty agreements
- Price points and form factors that clients could leverage on.



DEPLOYMENT SCENARIO – SERVICE PROVIDER

OATH SOFT TOKENS:
THREE TIER SERVICE PROVIDER MODEL



For further technical information, please contact services@visolve.com
Call: +1-408-666-4320 Visit: www.visolve.com

ViSOLVE
OPEN SOURCE SOLUTIONS

COMPARATIVE STUDY

Method	Password	OTP + Password	Digital Certificates/PKI
Advantages	Widely used and supported by the largest number of applications Technology easily understood by users	Two-factor authentication compatible with password based infrastructure: zero client footprint option	Bi-directional authentication Can provide two-factor. Non-repudiation
Disadvantages	Relies on human protection and management of the secret.	Requires possession of OTP generation software/hardware or access to a secondary channel for OTP transmission	Certificate management cost can be prohibitive for large user base. Heavy footprint to manage on client. Not compatible with small devices. Requires distribution of certificate/smart card to client.
Key Vulnerabilities	Brute force Man-in-the-middle/client insertion Phishing Over the shoulder Keystroke loggers	Man-in-the- middle/client insertion Phishing (reduced to one time action)	User override of warnings Client insertion (reduced)
Applicability	Lower risk environments Legacy environments No network usage or protected network usage	B2C Commerce Enterprise Security (VPN) Environments not suited for PKI (e.g. password based application infrastructure)	Highly secure environments Monetary or legal transactions where non-repudiation is a required feature Environments where mutual authentication is required.