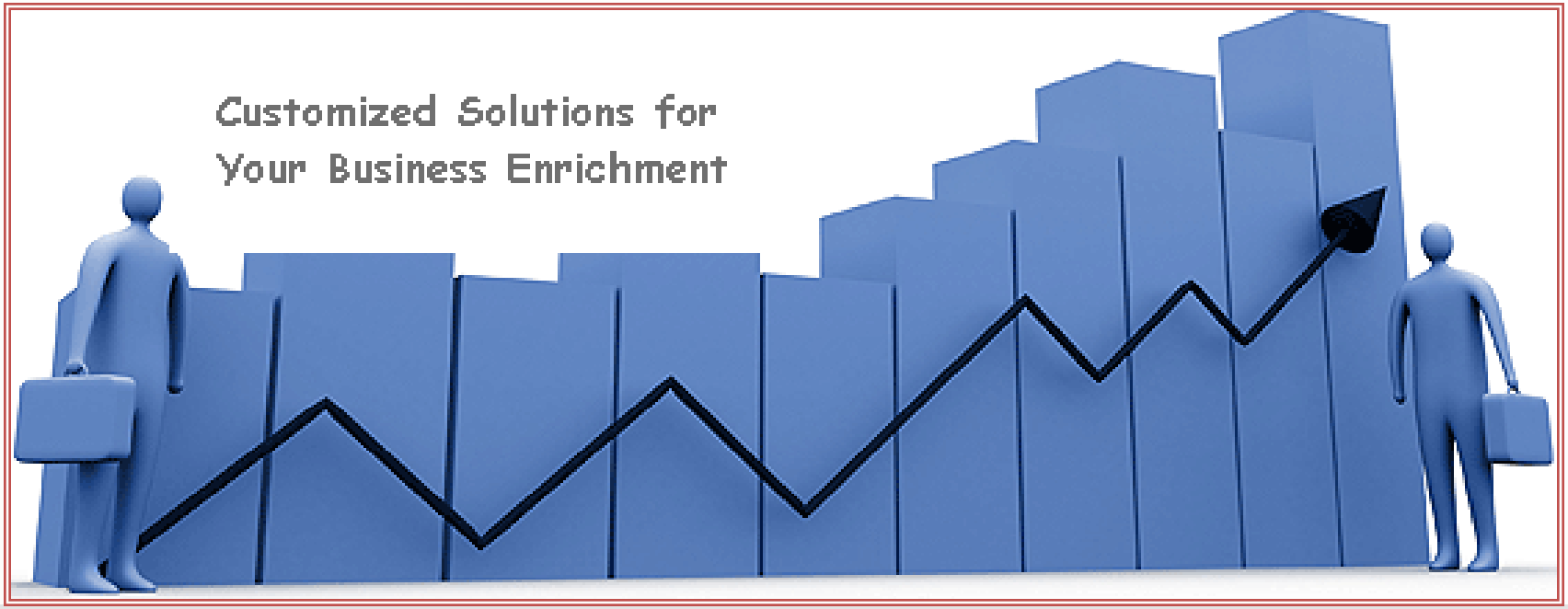
ViSolve
OPEN SOURCE SOLUTIONS

ViSolve – Open Source Solutions



Best-In-Class Authentication and Authorization Solutions & Services

© ViSolve Inc.

ViSolve – Securing Digital Assets

- Contents
  - Security Overview
    - Security Concerns
    - Security Needs
  - Technical Overview
    - Two – Factor Authentication System
    - OTP – One Time Password Solutions
    - OATH – Open Standards for OTP

Security Layers - Challenges

- Authentication
  - Ability to Validate
  - Proving Identity
- Authorization
  - Access to Network
  - Allowing to Transact
- Accounting
  - Management
  - Auditing
- Users
  - Profiling
- Security Policy
  - User Rights
  - Access Levels
- Security Platform
  - Applications Interface
- Security Device

Security Threats & Business Needs

- Vulnerabilities
  - Cyber Crime – Identity theft and Fraud
  - Phishing & Pharming attacks becoming more sophisticated and malicious

- Business needs
  - Enhanced Security: Stronger user authentication – Two Factor authentication System
  - Cost effective Password & Identity Management
  - Delivery Mechanism – Convenience of carrying security devices and ease of use

Power of One-Time Password (OTP)

- OTP deployment makes full life-cycle management easy & cost effective
- Flexibility and availability of various OTP methods – time synchronized, event synchronized or challenge response
- Password generated valid for single use
- Enhanced security environment for users to authenticate and transact on web
- Centralized repository of User profiles and credentials

ViSolve – Open Standards for OTP

- Today, with the exception of RADIUS, integration of OTPs can be achieved only through costly proprietary interfaces & protocols
- Can leverage on existing VPN/Wireless LAN infrastructure
- Low cost/no vendor lock alternative to proprietary solutions
- Easily added to existing web server password validation infrastructure
- Token based solution now inexpensive for wider B2C deployments

Technology Overview

HP–UX AAA Server and OATH:
Standard Based Two–Factor Authentication

Technology - Framework

- Two – Factor Authentication
  - Authentication using two independent method – typically something you have (device) and something you know (password)
- One – Time Password
  - Password valid for single use
    - Two-Party Model: Client and Server use OTP software or hardware to generate and validate password
    - Two-Channel Model: High value transaction can be authenticated by requiring an OTP being delivered through secondary channel vis email or SMS
- OATH
  - Open standards for OTP generation http://openauthentication.org sequence based algorithm
  - Supported by all of the token device vendors

Advantages of OATH vs. Proprietary OTP

- Low Cost
  - Sequence based algorithm allows low manufacturing cost for token device
  - No Royalty Programs
  - Leverage in both price-points and form-factors
- Wide variety of user deployment models
  - Standalone token device can be built into consumer electronics
  - Secondary channel solutions –SMS
- No Vendor Lock
  - Client, Server, user management components can be purchased separately
  - Multiple OTP clients can be concurrently supported from the same authentication server

Easy on Cost

Easy to Implement

Easy to End Users

Easy to Manage

OATH/OTP Authentication Opportunities

- **User Tokens**
  - Low priced tokens from multiple vendors
  - Soft-tokens that can run on java enabled device-mobile phones
  - SMS delivery of OTP for non java enabled devices
- **Mobile makes ideal OTP device**
  - Ubiquitous
  - Leverage applications provisioning to manage OTP soft-token
  - Addressing Consumer issue of handling multiple hard tokens
- **Opportunity for OTP authentication as telecom service**
  - Consumer authenticates to bank/retailer
  - Retailer authenticates password locally
  - Forward OTP to Service Provider

User – Base

Enterprise

Government

Medical

Finance

Web-Merchants

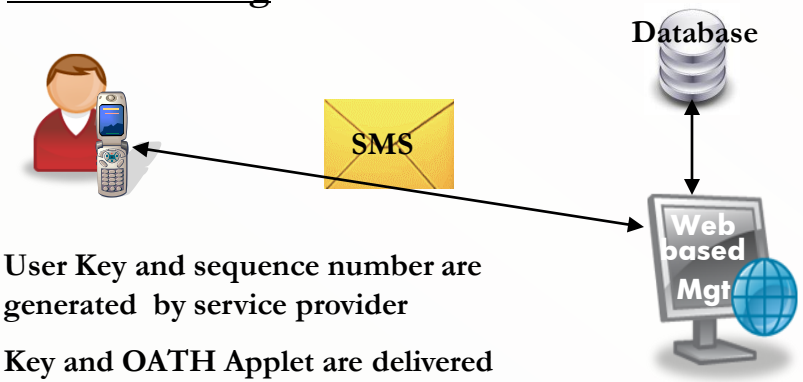
OATH/OTP Vs. Other Major Authentication Technologies

LOWER ← Cost/Complexity/Protection → HIGHER

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.

OATH Soft Tokens: Three Tier- Service Provider Model

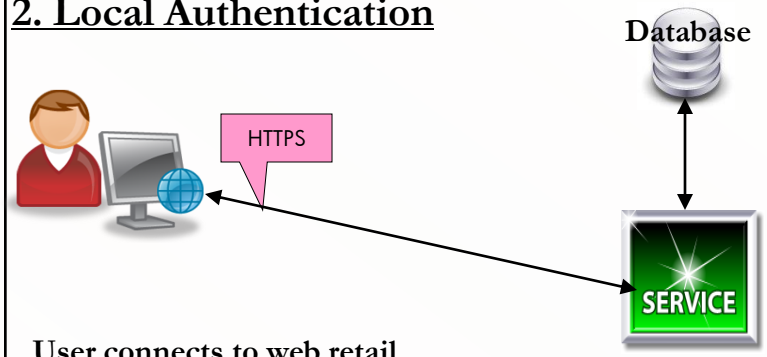
1. Provisioning



User Key and sequence number are generated by service provider

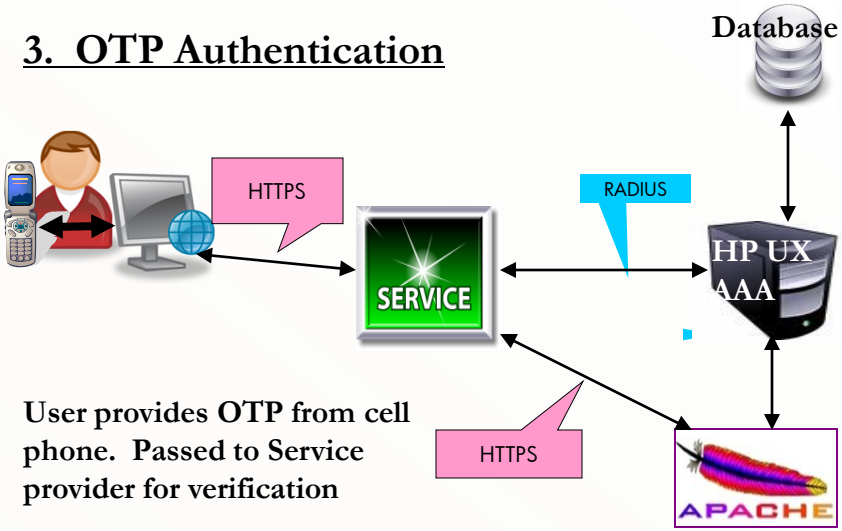
Key and OATH Applet are delivered to user device by client provisioning service.

2. Local Authentication



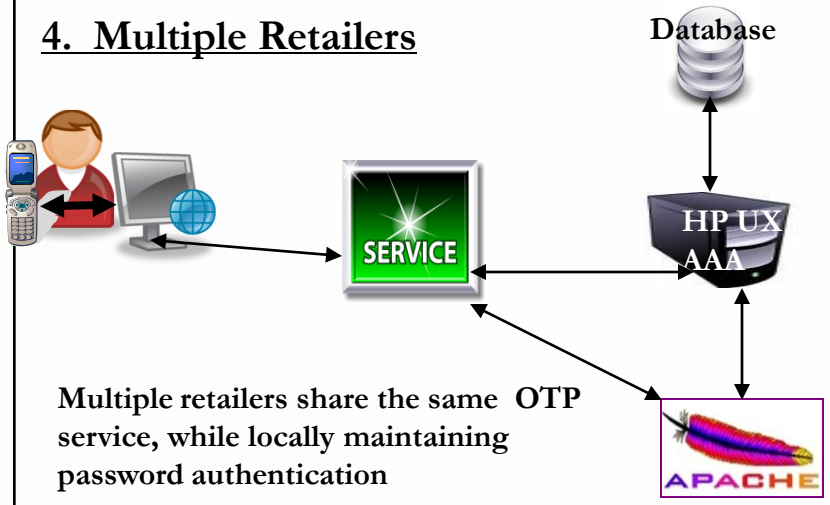
User connects to web retail presence via browser.
Password verified locally

3. OTP Authentication



User provides OTP from cell phone. Passed to Service provider for verification

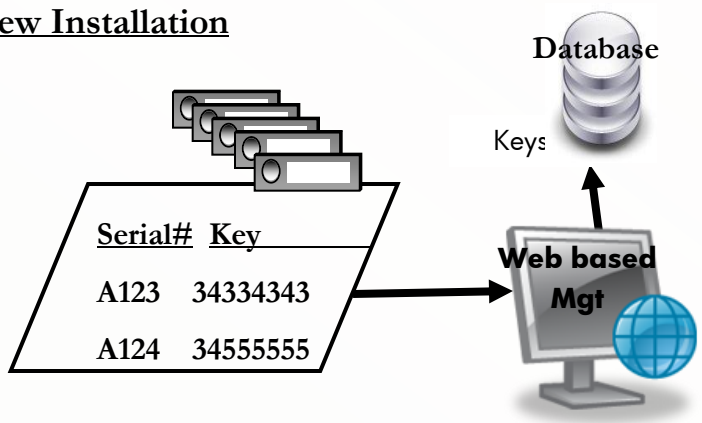
4. Multiple Retailers



Multiple retailers share the same OTP service, while locally maintaining password authentication

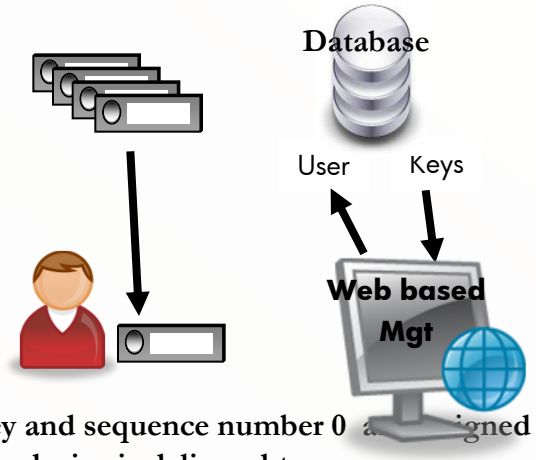
OATH: Provisioning Life Cycle: Token Cards

1. New Installation



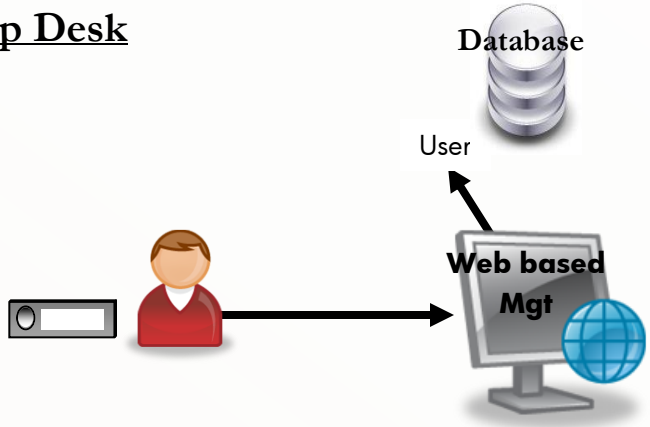
Supplier delivers tokens and key file. Admin tool imports serial number/key pairs into secure storage

2. New User



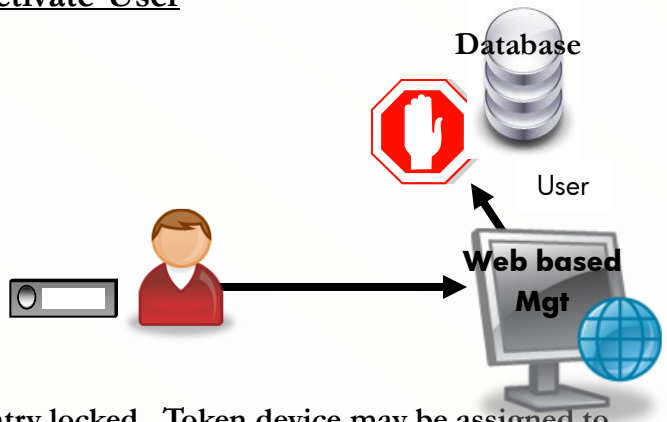
Serial number key and sequence number 0 a... igned to user entry. Token device is delivered to user.

3. Help Desk



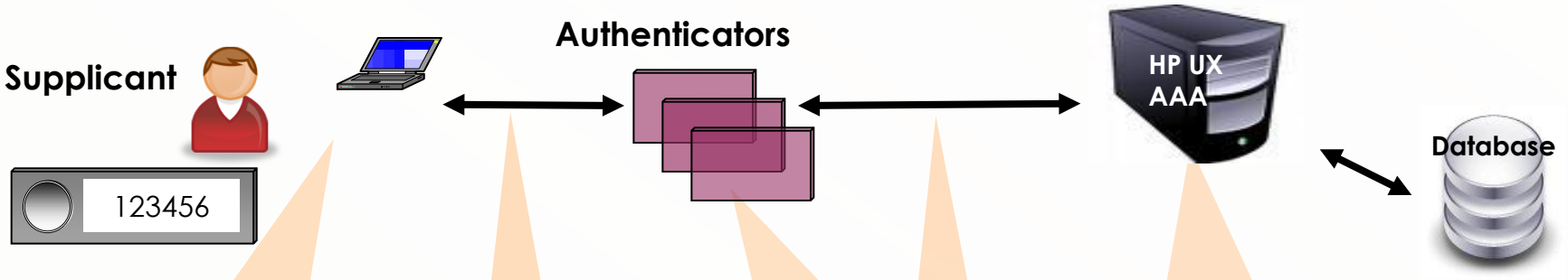
User entry can be resynchronized with user's token device if needed.

4. Deactivate User



User entry locked. Token device may be assigned to another user

Basic Password Authentication Sequence Adding Two Factor Authentication



1. User name/password entered on client device

   OTP appended to password field (separate prompt or combined with existing password input)

2. Protocol

   VPN: L2TP/ IPSec

   LAN: 802.1x

   Web: HTTPS

   …Etc.

3. Web Server, VPN Gateway, Firewall, WLAN Acess Point, Unix (login/SSH,…) etc

   Authenticate password locally or forward to AAA

4. Protocol

   RADIUS

5. AAA Server

   Authenticates password

   Tracks and logs user session

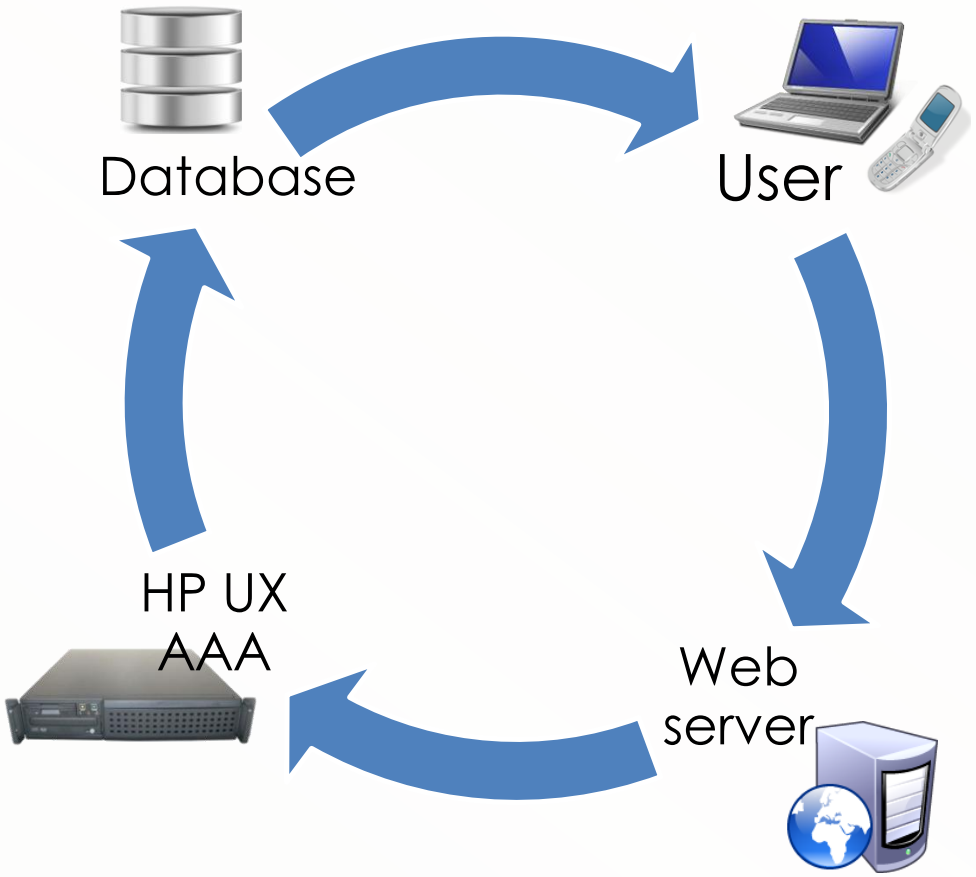
   OTP validated, token sequence number updated in Database)

Existing password based single factor authentication infrastructure.

Two factor authentication can be added with minimal disruption. Zero client software changes possible.

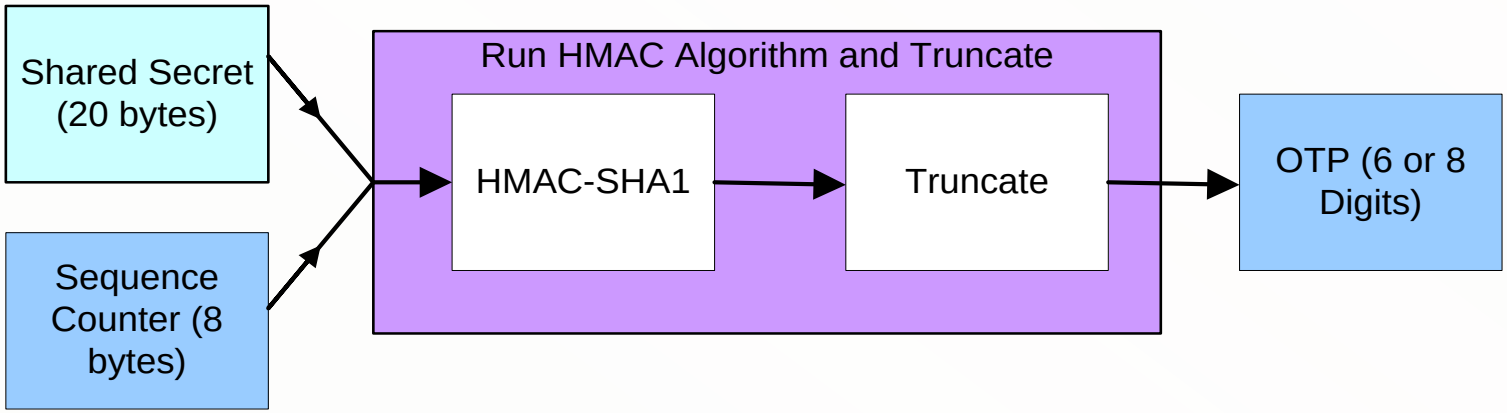
HP-UX AAA Server Overview

- **Purpose:**
  - Centralized service to provide authentication and recording of user access to network resources
  - Control access to wireless LANs, VPN gateways, http servers, and other RADIUS enabled devices or applications
  - Provides access and accounting control for greater security and compliance
- **Advantages:**
  - Based on widely supported RADIUS and Extensible Authentication Protocol standards
  - High performance/high availability features for enterprise and service provide deployments
  - Supports a wide variety of authentication methods including password, token cards and digital certificates
  - Highly customizable, supports ODBC compliant databases and LDAP compliant directories
  - Included with HP-UX11i

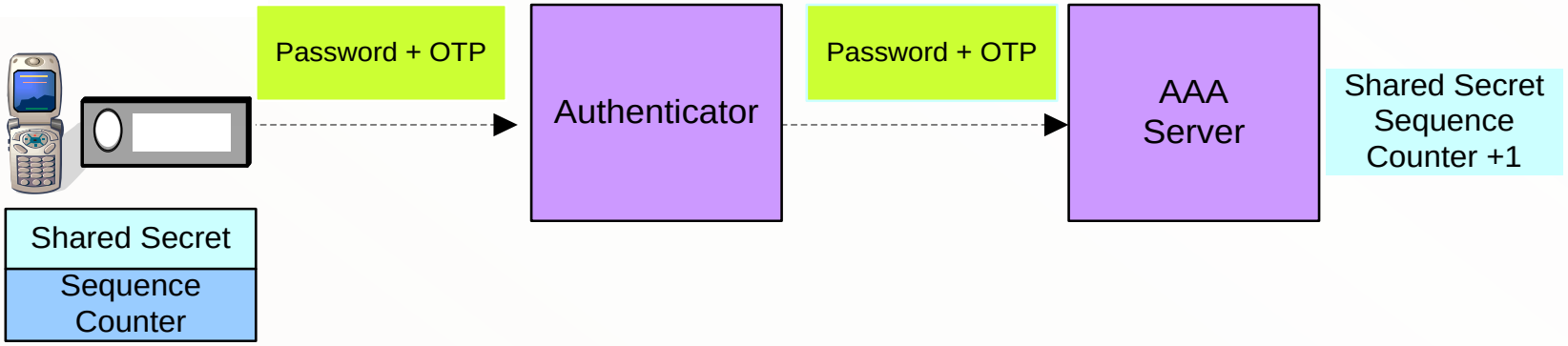


OATH: Higher level HMAC-based One Time Password Algorithm (HOTP)

Generate OTP



Validate OTP



Sample of Clients

F1000 companies, Technology Vendors and Healthcare IT Organizations

Thank You