

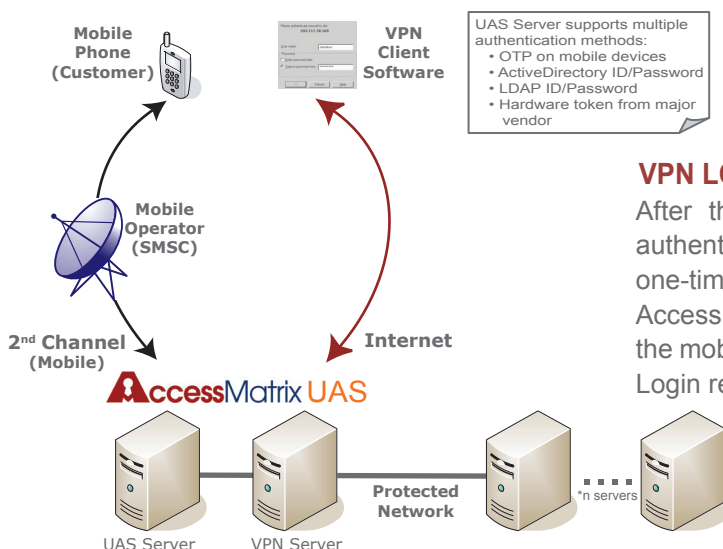
AccessMatrix™ Universal Authentication Server (UAS) enables organizations to deploy a wide variety of authentication methods to address the business requirements for strong authentication and evolving authentication mechanisms, through a single, unified framework.

Two Factor Authentication for secure VPN access using Mobile Phones, Pagers, PDAs and Tokens

AccessMatrix™ UAS One Time Password Module provides a complete and highly secure method of authenticating users. The mobile phone or mobile device with UAS solution becomes a Personal Trusted Device (PTD) to enable secure transactions via multiple delivery channels such as internet, phone, kiosk and mobile commerce.

This unique solution provides a convenient, secure and cost effective approach for secure VPN access by using Mobile devices and/or One Time Password tokens. For mobile devices, UAS-OTP leverages the GSM Short Message Service (SMS) to deliver a One-Time-Password (OTP) to the users' mobile devices for authentication. The architecture is based on the proven and patented AccessMatrix™ technology from i-Sprint to strengthen the existing ID/password authentication process during VPN logins.

UAS-OTP supports both existing security tokens and OTP using mobile devices for VPN access. The net result of this flexible solution is to help organizations protect their existing investment for tokens and eliminate the cost for additional tokens or replacements.



VPN LOGIN REQUEST

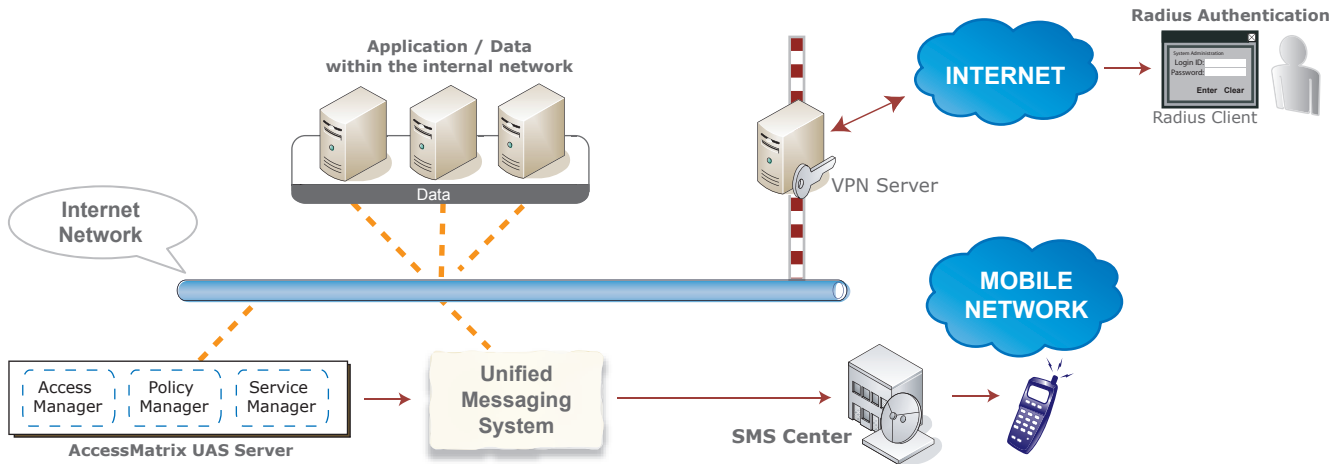
After the VPN Server has been configured to authenticate to the UAS-OTP server, a random one-time password (OTP) will be generated by the AccessMatrix security server and it will be sent to the mobile phone of the VPN user who initiated the Login request.

After the user has submitted the OTP information to the server, the AccessMatrix UAS-OTP server will compare the generated OTP and the OTP entered by the user. If the password is matched, the login transaction will be completed and audit trail information will be logged. If the password does not match, the user will be given the option to re-enter the correct password.

After a pre-determined number of retries, the login process will be cancelled and the events will be logged.

TECHNICAL ARCHITECTURE

The main components of the architecture are i-Sprint's AccessMatrix UAS-OTP Security Server, Unified Message System, SMS Centre and a mobile phone.



END-TO-END OTP LIFE CYCLE MANAGEMENT

AccessMatrix UAS OTP-VPN provides the functionalities to address the entire OTP life cycle:

- **OTP Configuration**

Administrators can configure the OTP characteristics via the Policy Editor (PE) and the following attributes can be specified:

- Expiry Time
- OTP Length
- OTP Format (Number, Alpha, Alphanumeric)
- Outgoing Message Template
- Delivery Channel
- Restriction to number of retries

- **OTP Delivery**

Administrators specify the delivery methods for the OTP either via SMS, email or any other methods supported.

- **OTP Validation**

UAS Server validates the OTP information for authentication purpose.

- **Audit Trail**

UAS Server provides comprehensive audit trail information to address the transaction audit requirements.

- **Reports**

AccessMatrix UAS provides a standard set of reports.

BENEFITS

Organizations will be able to provide a highly cost-effective, massively scalable strong authentication mechanism to allow for VPN access.

Further details about i-Sprint's products are available at www.i-sprint.com. To reach us, please email to enquiry@i-sprint.com or contact any of the offices or our resellers in your area.