Technical White Paper

AuthenTec Online
Open Authentication Whitepaper

About AuthenTec

AuthenTec is the world's #1 provider of fingerprint sensors, identity management software, and embedded security solutions. AuthenTec security and identity management solutions address enterprise, consumer and government applications for a growing base of top tier global customers. Already shipped on hundreds of millions of devices, the Company's smart sensor products, software and embedded security solutions are used virtually everywhere, from the PC on your desk to the mobile device in your hand to the server in the cloud. AuthenTec offers developers and users secure and convenient ways to manage today's rapidly evolving digital identities and security needs. AuthenTec is very interested in participating to the W3C Workshop on Identity in the Browser.

Security and convenience for you and your customers

AuthenTec Online OATH Services bring unparalleled privacy, convenience and security for your customers. While a plethora of tokens may be supported, in the most convenient case, users authenticate with a swipe of their finger. The Online Authentication Services provide all the high-level Internet security components and infrastructure while also delivering ease of integration with your site.

The user experience

Passwords are a pain. Simple passwords are bad for security. Tough passwords are bad for the user's experience. And passwords can be shared or phished, compromising the security and integrity of a customer's account. It's a lose-lose situation. AuthenTec delivers a winning solution by replacing passwords with the swipe of a finger. Remembering secure, complex passwords is a thing of the past! And by removing your reliance on passwords, password-related support costs can be eliminated!

Home Page
- User Id Pre-filled
- System Ready for authentication
- User is prompted to authenticate with a provisioned token. (E.g. swipe a finger, insert smartcard, plug-in USB vault, enter vault PIN)

Figure 1: User Authentication Experience

Online Tokens

While offline devices like OTP calculators are in principle usable, the primary focus of AuthenTec Online OATH is on "online tokens", i.e. tokens which are connected to the client computer.

A typical token suitable for the Online OATH is e.g. a fingerprint reader with OTP capabilities, a smartcard with OTP Java applet, or a USB token with OTP generator. Other secure elements (e.g. Intel ME, TPMs) can be used alone or in combination other factors such as facial recognition software.

Authentication

The user experience shown above is accomplished by a secure interaction between an OATH enabled web server and a client browser supporting the extensions noted in this document. Initially this service can be rolled out with browser extensions, later browsers may integrate the feature set directly.

1. **The Service Provider**: This is the online web service to which a user authenticates.

2. **The End User**: This is the user of the online service who needs to be authenticated.

3. **OATH Service**: This service verifies the OCRA on behalf of the Web Service (and provides DSKPP for Tokens – see below). It may be run in the backend systems of the service provider or hosted externally.

Authentication of a provisioned account is a matter of OCRA verification of a credential release from the client driven by javascript (communicating with the Authentication Token interface).

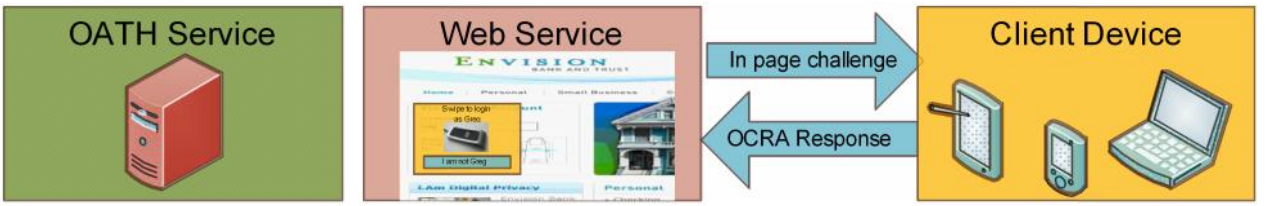

Figure 2: Communication for Authentication

To summarize the interaction in the steps shown above:

1. The End User needs to access protected content. A logon page is presented. The logon page contains embedded tags which cause the TokenList to be added to the DOM (document.TokenList) by the Online OATH compliant browser (initially via a browser extension). JavaScript in the page chooses the token(s) to interact with and presents an associated authentication UI.

2. For example, if the Fingerprint token has been provisioned, the traditional Login/Password area may be replaced with a request to "Swipe to Enter". A swipe of the finger will trigger the Token's callback function, providing the OCRA encoded response to the Service's challenge (set up by the web page).

3. The encoded data is made available to the JavaScript via the DOM – and may be sent to the server for verification.

4. The End User is given access to protected content or resource by the page assuming the response has been verified by the Web Server.

Provisioning

Before an End User can be authenticated as described above, they need to be provisioned by the web site. Each Token object in the TokenList has an associated "Provisioned" field and "Provision()" method to perform DSKPP with the OATH Service. The location of the OATH DSKPP compliant provisioning server is provided to a *Provision*() method.

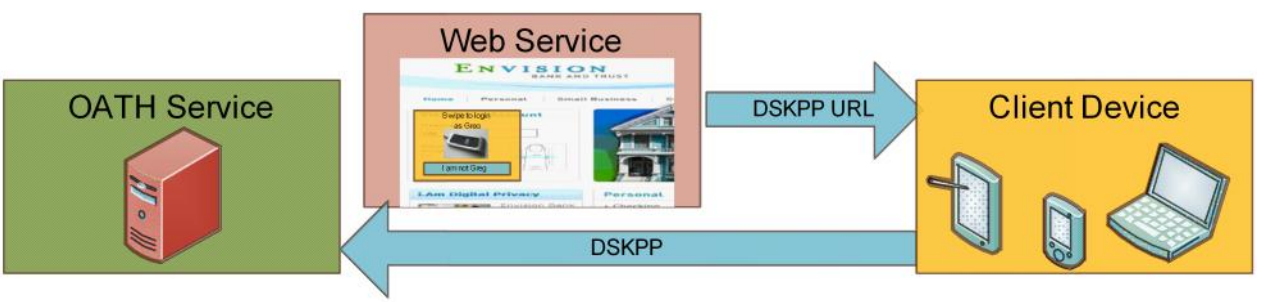

Figure 3: Online OATH Provisioning

A user of Online OATH may register to a web site without creating a user id. An option to create an account may be offered by the web server using Identity information from the user's public profile or the site may use standard User / Password Credentials for the initial verification.

Once logged in, provisioning for the user/client combination is accomplished in three steps:

1. Device Validation: The JavaScript verifies that a Token in the TokenList is "Enrolled". If not, enrollment may be initiated by the script before proceeding.

2. Token Authentication: The user is verified with the token (e.g. finger is swiped or PIN is entered as required by the token) to bind the user to the token and guarantee future OTP releases are

3. The OATH service provisions the token to the client via the plug-in and JavaScript using DSKPP (which encapsulates the user & client authentication achieved in step 1).

Provisioning is done once per user per web site per machine. The web site may decide to present its own interface for device management or leave it to the user to manage his vault.

Token Enrollment

Each Token object will also have an *Enrolled* field and *Enroll*() method to initially set up the token for a user as required. This step should only be required once per user per machine (or just once if the user has a portable Token). Token enrollment is unique per Token type. For finger print sensors, the enrollment process will record templates that can later be matched to an extraction. For "vault" devices like TPMs or Intel ME a PIN will be recorded for subsequent verification.

AuthenTec Setup

Enrollment

Figure 4: Enrollment

Identity Management

The base installation of Online OATH will include a “soft token” functionality via a “software vault” which makes use of the best security a platform can offer (Windows Secure Storage, Mac OS Keychain etc.). It will also include basic profile management for the end user to enable Web Server registration via Token based identification as well as management of the provisioned OTP seeds.

The TokenList properties in addition to a list of tokens will provide a list of Identity objects with standard properties. These may be used to populate registration fields with the user’s consent to facilitate more convenient binding of a meta-data to a web account.

Each Identity profile will similarly be bound to the token such that it’s release to a web site or modification is preceded by token authentication (human factor in the case of biometric tokens).

The identity and OTP seed management interface will be driven via an HTML5 compliant UI with data store access via a standard JavaScript API included as part of the specification.

Web Site & Server Integration

HTML tags specified by the standard will wrap the necessary DIV sections and JavaScript to verify the presence of Online OATH support in the browser and make use of its functionality.

Back-end integration
The OATH Service will be available via 3rd party providers conforming to standard interfaces as defined in RFC6063, RFC4226 and other OATH specifications.

An open source reference implementation may be included as part of the OATH Alliance offering for DYI solutions.

Token Providers

To date token providers (Fingerprint sensor manufacturers, facial recognition software, smart card manufacturers) have provided “Platform Drivers” for the machine on which they are installed. To facilitate their use in the online world, the Online OATH standard will include the necessary sample code for these manufacturers to install the necessary Token Drivers.
There will be coverage of existing standards such as PKCS11, MCAPI etc. in the base install to more easily pick up existing tokens support where available.

Further Information

For more information on the AuthenTec Online OATH proposal, please contact AuthenTec at Vito.Fabbrizio@AuthenTec.com.