initiative for open authentication

An Industry Roadmap for Open Strong Authentication

Initiative for Open Authentication

CONTENTS

Introduction

The Internet has enabled peer-to-peer communication and the exchange of information in an unprecedented way, transcending in a few years the geo-political barriers of yesterday's world. E-commerce and e-mail are two resounding examples of the transformation exerted by the "network of networks" on people around the globe. Unfortunately, the ubiquity and flexibility of the network has also brought its own set of challenges and security concerns, particularly in the area of user and device authentication. This white paper articulates the first step towards a strongly authenticated environment: It offers a vision and a straight-forward roadmap for propagating strong authentication across all users, all devices, all applications, and all networks.

The Need for a Strong Digital Identity

Although recent technology, communication, and geo-political developments (e.g., the rise in Web services, spam, and terrorism) point towards stronger network security, three network trends stand out as driving the need for strong digital identities: identity theft, the rise of federated identity networks, and the proliferation of IP devices.

Identity Theft Network Effect

In the 2002 Federal Trade Commission (FTC) annual study on consumer complaints, identity theft for the third year running was the most frequently cited reason why individuals contact consumer protection authorities. As mainstream consumer services such as banking, health care, and insurance complete their migration to the network, these complaints will only increase. Yet, the fundamental security mechanism used to protect personal information online remains fairly unsophisticated. An average person has more than a dozen passwords, which hackers using software programs can typically copy and crack in seconds. As credit card accounts, e-mail addresses, social security numbers, and many other kinds of personal information are increasingly used and stored online, precious information can more easily be stolen, from any place at any time. The "network effect" related to identity fraud creates the need for strong credentials. If "something you know" can be stolen through the network, only "something you have" can reduce the threat. In time, a security token in the form of a specialized device or integrated within traditional digital assistants and mobile phones will be the only viable solution for reducing the infinite points-of-attack threat posed by a global public network.

Rise of Federated Identity Networks

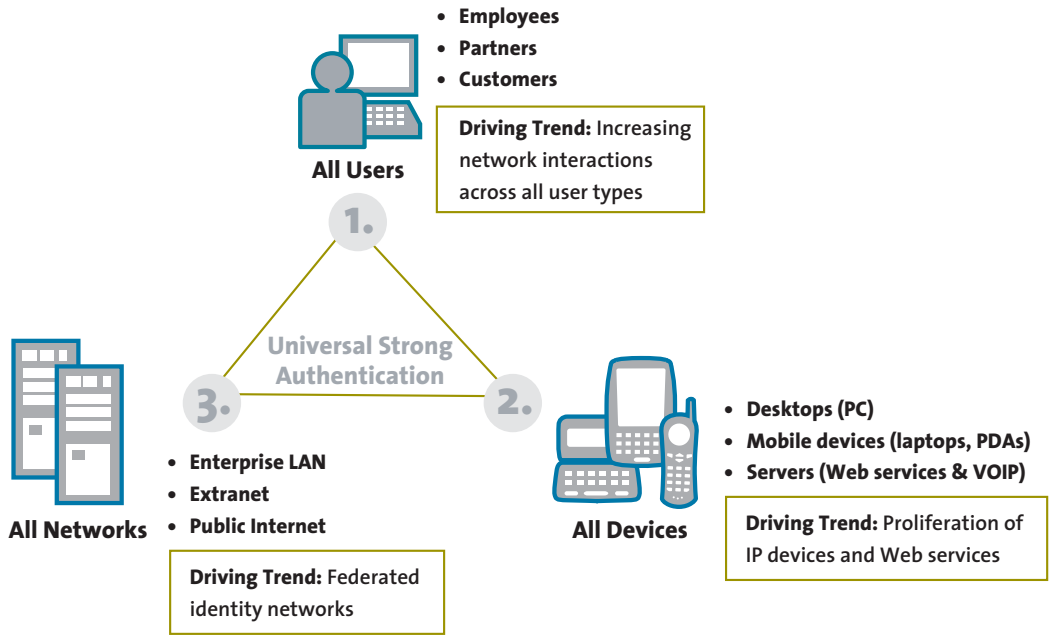
With the introduction of network-based systems for managing corporate content, supply-chain data, and customer services, enterprises are increasingly challenged to provide access to a very large and dynamic group of end users that includes remote employees, business partners, and customers. The complexity and cost of managing identities across internal and external systems, combined with the necessity of opening up access to data, has created the need for federated networks where identification, credentials, and attributes can be shared among partners. This convergence towards federated identity networks greatly accelerates the need for stronger identity. If the establishment of technical standards is an important prerequisite for sharing identities, trust is the fundamental business requirement. To authorize a transaction in a federated identity network, the relying party must be able to trust the credential and identity that was issued and verified by another entity. The strength of this identity must be asserted and evaluated against the recipient's security policies. When an identity is shared, its strength determines security across the entire access control chain, creating complex dependencies and liabilities across multiple business and legal parties. Therefore, the crucial issue of trust in federated networks can only be addressed through the pervasive and interoperable deployment of strong identity technology, security, and operation best practices.

Proliferation of IP Devices (Rogue Devices)

Security and trust in any network is a function of all the elements that make up that network. This includes end-point (client and server) devices that can impersonate users and organizations. As network devices (e.g., mobile phones, PDAs, portable digital music players, set-top boxes, TPM-based laptops) proliferate, the ability to distinguish between trusted and rogue devices is a fundamental security requirement. Because an authenticated device can act as the root of trust, it can also provide the security foundation for a new breed of applications (e.g., identity based anti-virus solutions and digital information rights management software). From this standpoint, device authentication is a core requirement of any strong identity management strategy.

Universal Strong Authentication for Users and Devices

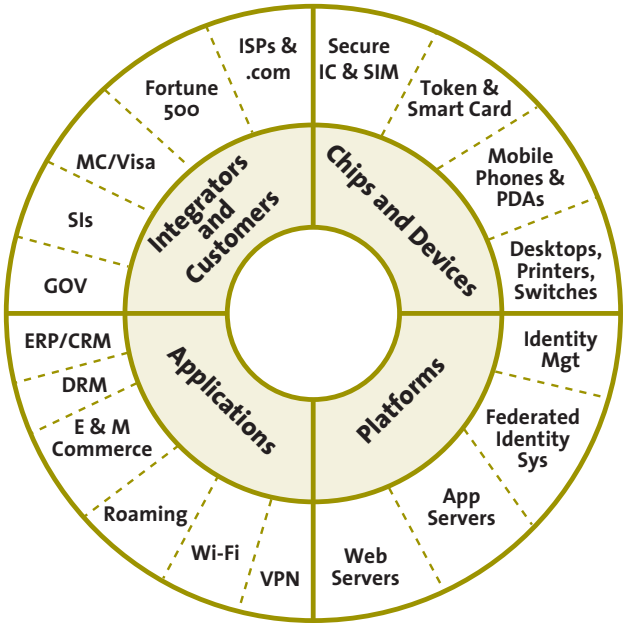
The strength—that is, the trustworthiness—of an identity depends on multiple factors. The initial authentication process (identity verification), the type of credential being issued (security token), and the depth of the relationship between the authenticator and the authenticated entity all contribute to the strength of an identity. Beyond the authentication process, the security policies enforced by the authentication authority—its operation best practices—have a direct impact, as well. Strong identity management must take into account technology, policy, and operational issues. For this reason, OATH believes that the voyage toward strong digital identity must start with strong authentication. Strong authentication is the first pillar of trusted networks where identities can be securely shared and trusted across independent partners. It is the foundation for a more secure network, where all people and all devices are strongly authenticated in an open, interoperable, and federated environment.



Strongly Authenticating Everyone and Everything—Everywhere

Realizing the Vision

To drive adoption of strong authentication across the entire user community—from corporate employees, to Internet users, to people accessing everything from health care records to government services—the industry must collaborate to lower the complexity of and financial barriers to strong authentication. Open technical standards and deployment profiles that promote interoperable solution components are powerful mechanisms for lowering complexity and cost. Therefore, the development of an open and royalty-free specification for strong authentication will be OATH's initial focus. Open, universal strong authentication is intended to provide all key constituencies (device manufacturers, identity management vendors, security service providers, and application developers) with a common framework for strongly authenticating users and devices.



Open Strong Authentication Ecosystem

Open authentication aims at the following goals:

- Establish an open reference architecture for strong authentication by leveraging existing open standards when possible, and otherwise leading standardization efforts through well-established technical standard bodies.
- Proliferate low-cost, multi-function authentication devices (e.g., tokens, smart cards).
- Transform today's mobile devices (e.g., cell phones, PDAs, laptops) into strong authentication devices.
- Propagate device credentials, strong authentication algorithms, and authentication client software across many network end points (e.g., desktop computers, servers, switches, Wi-Fi access points, set-top boxes).
- Build around well-established infrastructure components such as directory and RADIUS servers.
- Facilitate native support (platform connectors) for strong device and user authentication in application development and identity management platforms.
- Leverage federated identity protocols as a powerful propagation and integration mechanism.
- Increase the breadth of packaged applications (e.g., enterprise resource planning (ERP), material requirements planning (MRP), customer relationship management (CRM) application connectors) that support strong authentication.
- Enable best-of-breed solutions through interoperable components.

To be effective, a specification must be jointly defined and published by key industry partners that share the vision of universal strong authentication. By laying the ground for ubiquity, integration, and interoperability, an open architecture can decrease the risk and complexity of deploying strong authentication products. In turn, the promise of reduced risks and costs will drive adoption across enterprises, service providers, and governments around the world. Ultimately, by making strong authentication (all users, all devices) part of the network fabric, the entire user community will benefit. Last but not least, by increasing the trust of the network end points, new types of secure interaction will become possible.

The OATH Roadmap

To initiate and facilitate the collaborative development process, OATH has created an initial roadmap. From a technical architecture standpoint, the proposed roadmap draws attention to three main areas:

- Credentials and security devices
- Authentication protocols framework
- Credential provisioning and validation

Credentials and security devices

Open authentication must address the three major authentication methods:

- Subscriber identity module (SIM) -based authentication (using GSM/GPRS SIM)
- Public key infrastructure (PKI) -based authentication (using X509.v3 certificate)
- One Time Password (OTP) -based authentication

These three methods specify the core set of authentication credentials (SIM secret, X509 certificate, and One Time Password). The roadmap calls for this core set of credentials to co-exist and interoperate across devices and applications.

Each of these methods has a specific use in an open and interoperable environment:

- **SIM-based authentication** – This authentication method predominates in telecommunications, and is emerging as an important authentication method in public Wi-Fi networks (authentication and roaming across GSM/GPRS and 802.11 networks).
- **PKI-based authentication** – PKI is a fundamental security component of all major Internet protocols for authentication and communication (e.g., Transport Layer Security (TLS), WS-Security, IPSec IKE, 802.1x, Session Initiation Protocol (SIP)). The choice of X509 certificates as strong credentials is also consistent with deployment trends in enterprise and government markets. Furthermore, certificates offer additional security functionality beyond authentication (e.g., for form and e-mail signing and file encryption).

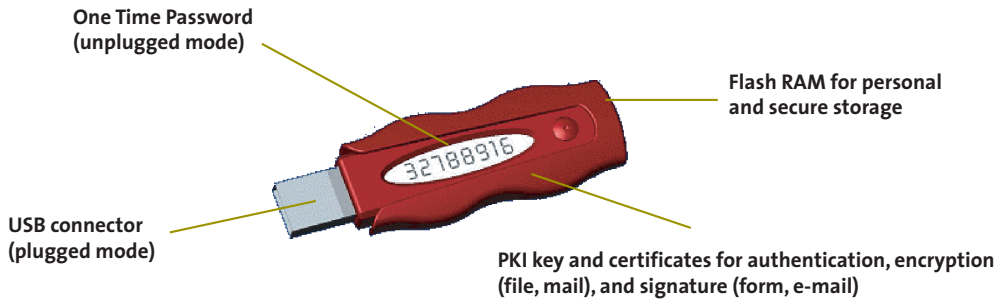
- **OTP-based authentication** – This method is intended to act as a bridge between legacy and modern applications. OTP credentials will facilitate integration with applications that rely solely on user passwords (e.g., Web applications, mainframe applications, and ERP systems). Because end users are already familiar with static passwords, a device-generated password can greatly facilitate the transition to stronger authentication (for one thing, the application user interface does not change). Therefore, support for OTP is essential to the successful propagation of strong authentication.

Because there is no established OTP open standard, the roadmap proposes a common OTP algorithm. The algorithm will be open-sourced and used as the base OTP algorithm for soft and hard security tokens. OATH has already investigated an event asynchronous algorithm for this purpose and determined that it is a good candidate for an open OTP standard.

All-in-one security devices

A major goal of the roadmap is to foster the creation of security devices that can embed many if not all the base authentication methods. The intent is to create highly flexible and versatile security devices (e.g., for authentication, encryption, signing, secure storage, and physical access). Comprehensive functionality and personalization (e.g., personal storage) are essential to influence users to embrace security devices such as a token on a key chain or a smart card in a wallet. By supporting multiple strong authentication methods, the same device becomes capable of interacting with a wide range of networks and applications.

The following remote access scenario illustrates the benefit of integrating multiple authentication methods into one single security device (e.g., a USB token with either a PKI-enabled SIM chip inside or a smart card, with a display integrated within the reader to display the OTP). With this hybrid device, a user roams over a Wi-Fi network using SIM-based authentication. Once on the public network, she can initiate a virtual private network (VPN) connection to a corporate gateway using her RSA private key and certificate, which are stored in the token. Once the VPN tunnel is established, she can log on to her company's portal to access a 401K account through a Web interface, using the One Time Password generated by the token. As demonstrated in this scenario, an open approach can break down the barriers created by proprietary devices in favor of a highly versatile token or smart card, capable of supporting very rich use cases.



An Example of a Hybrid Device

The roadmap proposes standard device profiles to allow chip and device manufacturers to produce back-end-compatible security devices. OATH intends to describe the common firmware and desktop APIs required for exposing authentication and device management functions (e.g., user PIN, serial number, key, certificate management) for the three base authentication methods. OATH will leverage existing or emerging industry application programming interfaces (APIs) when such standards already exist (i.e., CSP/CAPI, CCID).

Authentication Protocols Framework

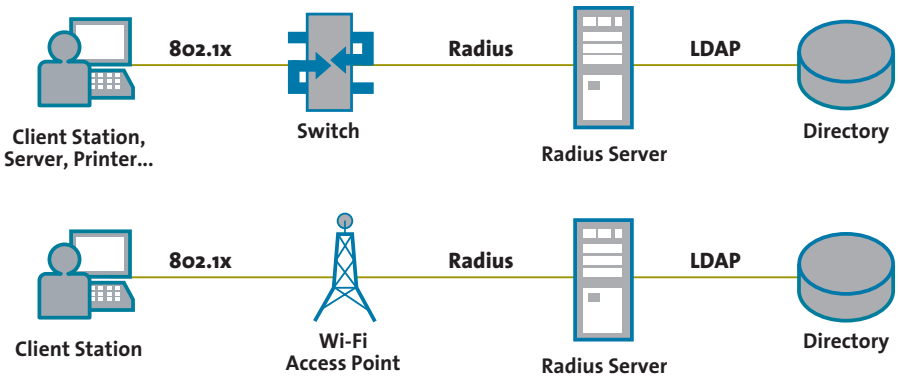
In many cases, the specific application dictates the authentication protocol. For example, in a Web application, TLS will often be the primary protocol. In the VPN case, IPSec IKE is the standard, and for Wi-Fi (802.1x), Extensible Authentication Protocol (EAP) methods such as EAP-TLS or EAP-PEAP are the norm.

802.1x for network applications

For future network access applications, OATH will propose 802.1x as the authentication protocol framework. This is true both for wired and wireless networks (the authenticator is the access point for wireless networks; it is the layer-two switch for wired networks). 802.1x is a natural candidate because it already defines EAP methods for each of the proposed base authentication methods (EAP-SIM for SIM-based authentication, EAP-TLS for PKI-based authentication, and EAP-PEAP for OTP-based authentication).

802.1x for device authentication

The 802.1x framework is crucial to promote a consistent deployment profile for device authentication across manufacturers and OS vendors. OATH envisions the deployment of embedded 802.1x clients to enable these devices (e.g., VOIP phones, access points, switches, servers) to transparently authenticate to the network, before being handed an IP address and being granted access to the network.



802.1x As a Device Authentication Framework

Manufacturing-time device credentials

OATH foresees device certificates being combined with emerging secure com puting technologies such as the Trusted Platform Module (TPM) and the 802.1x authentication protocol framework. This convergence will foster a common technology stack and deployment profile, allowing device manufacturers to enable turnkey strong device authentication solutions. In fact, using the established profile, manufacturers and OEMs will be able to rapidly collaborate to embed the necessary hardware credentials and client software at manufacturing time.

Web service protocol for business-application integration

Universal strong authentication must address the protocol dichotomy between network access applications (dial-up, VPN, Wi-Fi) and business applications (Web or enterprise portals, Web applications, ERP systems, Web services). The 802.1x framework is particularly well suited to the former, but not to the latter. A Web service interface is better adapted to today's business applications. Because the authentication protocols constitute the primary mechanism for integration into applications, open authentication requires a palette of protocols that can support both types of applications. This requirement leads to the definition of a Web service API alongside the 802.1x EAP methods already covered. OATH proposes a Simple Object Access Protocol (SOAP) API that will leverage the WS-Security specification as the primary mechanism for encoding the base security tokens (OTP, X509 certificate), and will define a challenge-response mechanism for SIM-based authentication.

In summary, OATH endorses a dual interface model that is adapted both to the requirements of network access and the needs of higher-level business applications.

Application connectors and authentication clients

The main motivation for standardizing the authentication protocol and promoting the development of authentication clients is to foster the creation of application "connectors". Application connectors, or, agents are the client libraries of strong authentication. They must be portable across major operating systems and offer APIs across popular languages. Such flexibility will make it easy for application developers to integrate strong authentication within custom applications (link, compile, and run). This is mainly true for the EAP protocols because the Web service can immediately leverage the Web services stack that exists in all major development platforms.

OATH will foster the creation of open-source projects for creating 802.1x clients that support EAP-SIM, EAP-TLS, and EAP-PEAP across multiple device operating systems, from cell phones and PDAs, to printers, Wi-Fi access points, and switch operating systems.

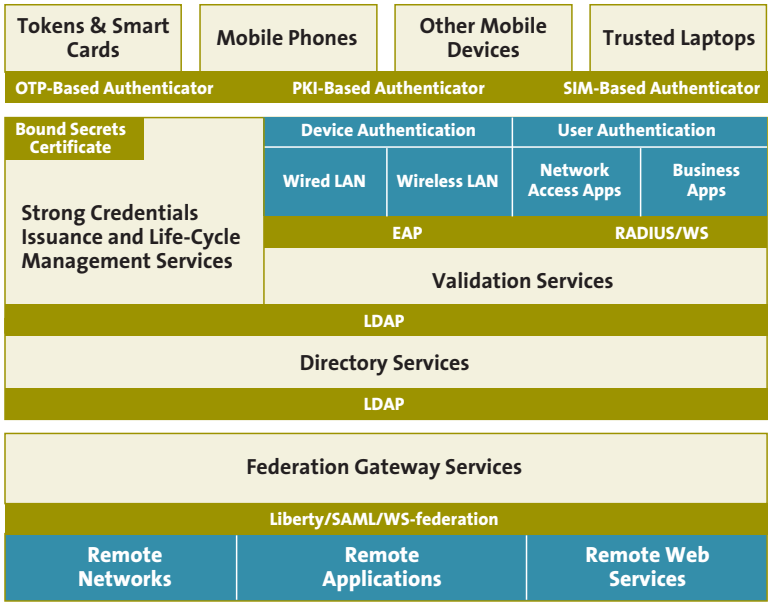
Credential Provisioning and Validation

Because universal strong authentication is the key objective, the blueprint needs a method to harmonize credential issuance and other lifecycle management functions across all types of secrets (symmetric keys or RSA key pairs). In the proposed method, the SIM and OTP secrets become subordinate to an RSA key pair (a device certificate key pair). The shared secrets are encrypted and embedded as attributes within the certificate. The certificate acts as a private store for the shared secrets, and the security device acts as a secure hardware vault for the "root" credential.

This approach will allow manufacturers and customers to leverage the breadth of secret management capabilities and security practices (e.g., key escrow, secure roaming, directory services) from existing PKI platforms. The method applies both to secure device personalization (shared secret and device certificates embedded at manufacturing time) and secure provisioning of user credentials. This unified credential lifecycle management framework will leverage existing public key cryptography standards and modern protocols such as XML Key Management Specification (XKMS).

Validation profiles will be defined by the choice of authentication protocols, as described earlier. Additionally, validation services will be able to validate X509 certificates using certificate revocation lists (CRLs) and industry standards such as Online Certificate Status Protocol (OCSP) or XKMS. OATH derives an additional benefit from leveraging 802.1x and the base EAP methods: Validation servers in a strong authentication environment have the same characteristics as RADIUS servers. This is a conscious choice, as RADIUS servers are already a key component of an ISP or enterprise network infrastructure. Furthermore, high-quality RADIUS servers are widely available from vendors and open-source projects. By leveraging the large existing installed base of RADIUS servers, OATH hopes to reduce the complexity and cost overhead for deploying strong authentication.

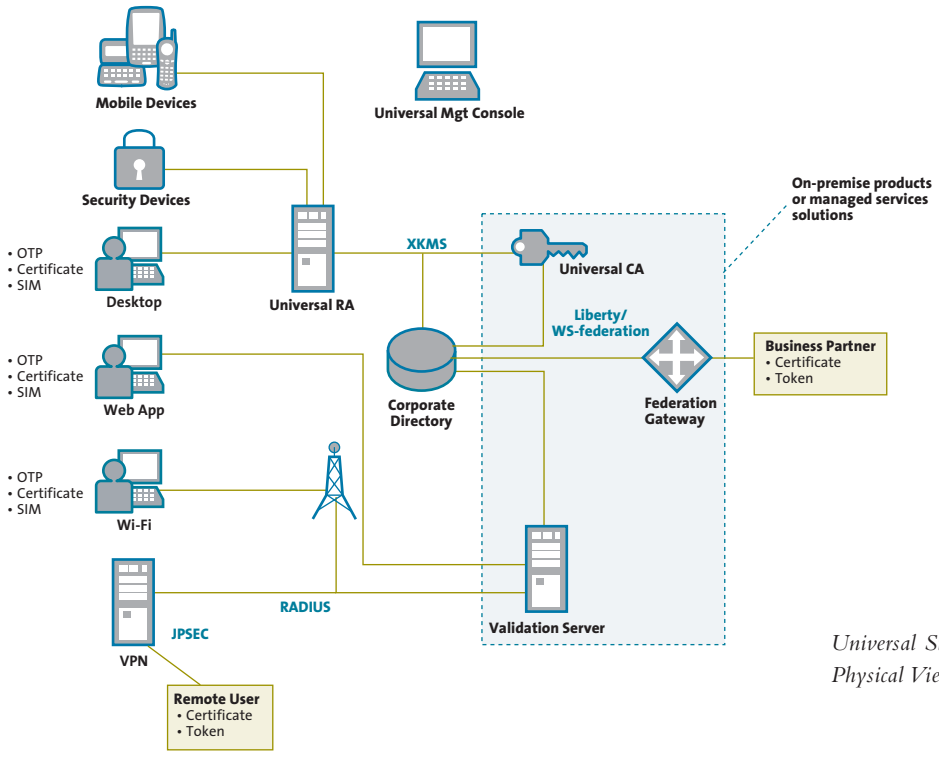
For applications that require a Web service interface, the validation server will be required to implement the SOAP validation protocol outlined in the roadmap. In the network world, the strong authentication validation server is congruent to a Radius server; in a service-oriented architecture, the validation server is an instance of a Web service. Because credential validation is highly complementary to credential mapping and exchange, OATH envisions consolidation of the validation Web service with the architectural concept of Security Token Service (STS), defined by Web Services Trust Language (WS-Trust), as an essential element in the roadmap.



Universal Strong Authentication - Logical View

An important architecture goal for universal authentication is to enforce the separation between validation and identity stores. OATH recommends that all identities (user or device identities, as well as device-to-user bindings) be maintained outside the validation server. This separation is important from an integration and cost-control standpoint. It promotes a distributed architecture that favors the reuse of an enterprise's existing infrastructure (e.g., corporate directories). In such architecture, the validation server is a minimal front end. OATH assumes that LDAP is used to enable the validation server and the directory to exchange information.

OATH also envisions a network where the device and the user authenticate only once to the "local" network (e.g., an enterprise LAN, an ISP). Once this dual strong authentication event has occurred, the device and the user would be able to seamlessly access a remote network or service without having to re-authenticate (federated and strong single sign on (SSO) for users and devices). In fact, OATH assumes that the remote service would leverage federated identity protocols to exchange authentication assertions and identity attributes with the entry point directory. To facilitate the exchange of identity assertions, OATH promotes the use of a federation gateway that can turn the local on-premise directory into a remote identity provider that can communicate authentication events to authorized external parties. Indeed, federated identity is an important architectural component of OATH as it can enable an external application to federate a strong credential without requiring that application to actually integrate or see the strong credential.



Universal Strong Authentication – Physical View

Conclusion

This white paper outlines the initial steps towards authenticating every user and every device, on all networks, using any strong credential. By approaching the problem holistically, OATH expects strong authentication to propagate deep into the network infrastructure and across all major applications and devices.

The first step for making strong authentication ubiquitous is the collaborative development of an open strong authentication specification that can be adopted across the industry. To that end, the authors presented an initial roadmap. This roadmap is intended to provide a starting point for designing an open architecture. In turn, the resulting open architecture and existing standards will provide the foundation for interoperable solutions that can be deployed across devices, identity management platforms, and networks.

The shared goal of strong federated identity has already attracted key industry partners. From that standpoint, this white paper is also a call to action to join OATH in its efforts to develop an open architecture and to create innovative solutions based on that architecture.

For further information regarding the participation of your organization in this effort, please contact OATH, the Initiative for Open Authentication, at www.openauthentication.org.