



WHITE PAPER

Standards-Based Shared Authentication for Scalable Consumer Authentication: Behind the Technical Curtain





CONTENTS

+ Introduction	3
+ Standards-Based Shared Authentication Network	4
+ Scalable by Definition	5
+ Common Misconceptions About Standards-Based Shared Authentication	6
+ Summary	7
+ About VeriSign	7



Standards-Based Shared Authentication for Scalable Consumer Authentication: Behind the Technical Curtain

+ Introduction

Many organizations recognize the need to deploy a two-factor consumer authentication solution in order to mitigate risk, maintain compliance, and satisfy consumer demand for secure transactions. However, they often find that isolated managed services, proprietary networks, or in-house solutions limit scalability and force customers to keep track of a separate credential for every website on which they conduct high-value transactions. Forward-looking organizations are deciding that a standards-based shared authentication network is the only viable option for quickly, cost-effectively scaling consumer authentication and encouraging widespread adoption of online services.

The following chart identifies key differentiators of the leading consumer authentication models. These differentiators impact the scalability and ease of use of consumer authentication solutions.

SOLUTION TYPE	HOSTED / MANAGED	PART OF A NETWORK	NUMBER OF CREDENTIAL TYPES	BASED ON OPEN STANDARDS
Proprietary network	Yes	Yes	Proprietary tokens only	No
Isolated managed service	Yes	No	Depends on the solution	Depends on the solution
In-house consumer authentication	No	No	Depends on the solution	Depends on the solution
Standards-based shared authentication network	Yes	Yes	70+ OATH member credential types	Yes

- A **proprietary network** includes multiple organizations on its network, but requires all organizations to use authentication infrastructure and credentials manufactured by a single vendor. Only organizations with the proprietary components can participate in the network.
- An **isolated managed service** frees organizations from building and maintaining an in-house consumer authentication solution, but it does not enable participation with other organizations.
- An **in-house consumer authentication** solution is built onsite and does not enable participation with other organizations.
- A **standards-based shared authentication network**, discussed below in more detail, is a managed service based on open standards.

+ Standards-Based Shared Authentication Network

A standards-based shared authentication network enables multiple organizations to share a single, third-party infrastructure for authenticating second-factor credentials such as one-time passwords (OTPs).

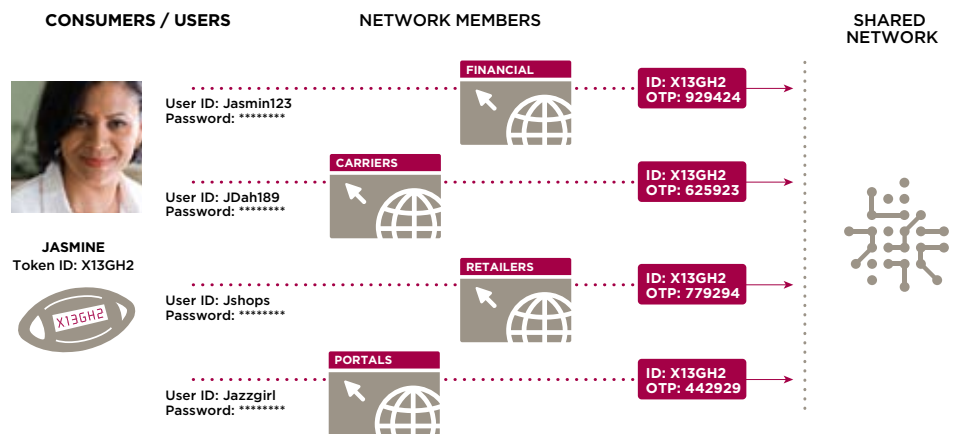
This approach benefits both users and organizations:

- **Users** – A standards-based shared authentication network simplifies the user experience and encourages consumer adoption by allowing users to employ the same authentication credential with every organization on the network.
- **Organizations** – A standards-based shared authentication network minimizes deployment costs and increases scalability by allowing organizations to offer two-factor authentication without investing in authentication infrastructure or having to distribute or manage credentials.

To enable two-factor authentication, organizations simply use a Web services application programming interface (API) to communicate with the third-party vendor’s authentication infrastructure. As a hosted service, all authentication processes occur “in the cloud,” without requiring additional investments in hardware or software. Organizations can start out by accepting credentials from other sites on the network. Then, as adoption increases, they can begin offering their own branded credentials to some or all of their customers.

Because it uses open standards, a standards-based shared authentication network allows organizations to easily join the network, regardless of hardware or software. That is, they do not need to buy proprietary products. This model also allows users to authenticate themselves using any standards-based (e.g., the Initiative for Open AuTHentication (OATH) credential or token—whether issued by the organization, another organization on the network, or a third party.

Figure 1: Consumer Experience with a Shared Two-Factor Authentication Network



+ Scalable by Definition

Standards-based shared authentication enables organizations to easily scale users, types of online services, form factors, and network relationships. It also drives adoption of two-factor authentication by making it accessible to more organizations and streamlining credential usage for customers, similar to the way ATM usage increased when banking customers could use their bank's ATM card at another bank's ATM via a common network.

Standards-based shared authentication provides scalability in the following dimensions:

- **Time and total cost of ownership** – Standards-based shared authentication is a hosted service. Because organizations do not have to implement, manage, or maintain an in-house authentication infrastructure, they can offer strongly authenticated online services with minimal investment of time or money—both at the beginning of deployment and over time. Organizations don't even have to distribute credentials if their users already have a standards-based credential or obtain one from a third party.
- **Scope and complexity** – A standards-based shared authentication network enables organizations of any size to participate in an ecosystem that expands exponentially as new entrants join the network. By managing the complexity of authentication across the network, creating a trusted environment, and enabling credential/token-sharing among organizations, the network helps organizations accommodate a growing number of business relationships, customers, and services.
- **Ease of use** – Today's consumer has the burden of not only remembering dozens of passwords but also carrying multiple authentication credentials in order to conduct business online. Standards-based shared authentication simplifies the problem of multiple credentials by enabling the use of a single credential across multiple sites, similar to the ATM networks.
- **Reliability and availability** – Networked consumer authentication solutions must be able to handle security for millions of users. A standards-based shared authentication network operates on a global, carrier-grade infrastructure that meets the industry's highest levels of availability and builds in multiple redundancies. Few organizations have the resources to deploy and maintain an infrastructure of this size and stability.
- **Innovation and interoperability** – Because a standards-based shared authentication network is based on the OATH standard, consumers can use a variety of tokens (at a range of price points), and organizations are not locked into a specific solution that requires proprietary components. They can leverage existing network and application protocols to more quickly integrate online applications and multiple credential solutions into the validation network.



+ Common Misconceptions About Standards-Based Shared Authentication

Because a standards-based shared authentication network engages multiple organizations and touches many consumers, some organizations make erroneous assumptions about risk, liability, and complexity.

MYTH Standards-based shared authentication will...	FACT Standards-based shared authentication enables companies to...
Decrease my control of the user experience.	Maintain control of the user experience while expanding value, services, and choices for customers.
Burden customer support and maintenance staff with tasks associated with one-time passwords (OTP).	Provide easy-to-use credentials to a growing number of users—without installing client software or adding customer support personnel.
Jeopardize my customers' security and confidentiality.	Provide consumer authentication services without sharing customers' personal data with other companies on the network.
Complicate the user experience.	Simplify the user experience by enabling the use of a single token for all transactions on the network.

Control of User Experience

Organizations that use a standards-based shared authentication infrastructure maintain complete control of the user experience and security policies. Security and user interface parameters are separate from the actual credential validation steps, so each organization's online applications manage the first authentication factor—usually a user name and password—in their own user database. For example, each organization maintains its own policies about lost tokens and who is allowed onto its network. Organizations only share the second factor of validation. They do not share liability.

Minimal Impact on Customer Support

A standards-based shared authentication network allows organizations to scale the number of users without adding support personnel for customer service, software upgrades, or infrastructure maintenance and management—especially if the organization does not issue its own credentials. When carefully designed as a customer-facing service, two-factor authentication is intuitive and easy to use. OTP credentials do not require software installation or configuration by the user.



Security and Customers' Personal Data

Organizations using a standards-based shared authentication network do not share their customers' user name, password, or other personally identifying information with other participants in the network or the validating infrastructure. In addition, customers do not have to use the same user name and password at every site. All that is shared and validated is an anonymous credential and a corresponding OTP. For this reason, customer privacy and data protection laws are not an issue.

User Experience

A standards-based shared authentication network addresses a key barrier to widespread consumer adoption of two-factor authentication by simplifying the user experience. Customers can use a single credential on multiple sites, making it convenient and easy-to-use as part of their daily online lifestyle.

+ Summary

Standards-based shared authentication enables organizations to scale users, services, and relationships quickly and cost-effectively by providing a managed network for two-factor consumer authentication and token distribution. Contrary to popular misconceptions, standards-based shared authentication allows organizations to maintain control of their customers' personal data, the user experience, and security policies while simplifying the user experience and minimizing impact on customer support.

+ Learn More

For more information about VeriSign Identity Protection, please call 650-426-5310 or email: identityandauthenticationservices@verisign.com.

+ About VeriSign

VeriSign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

Visit us at www.Verisign.com for more information.