

# 2009 Trends in Strong Authentication Survey

## Survey Research Brief

*Sponsored by*



10 Maguire Road, Building 4

Lexington, MA 02421-3120 USA

[www.imprivata.com](http://www.imprivata.com)

## Research Brief

### 2009 Trends in Strong Authentication Survey

The national survey targeted executives across an array of industries including healthcare, financial services, state and local government agencies and others to understand how organizations are using technologies for secure authentication. This online survey was conducted via Zoomerang, an online survey services provider, and polled 237 healthcare IT decision makers and executives. The survey has a +/- 6 percent margin of error.

#### Key Findings

#### **Strong authentication and single sign-on (SSO) drive organizational cost-efficiencies, security and employee productivity**

86 percent of respondents stated that strong authentication is part of their SSO identity management solution strategy. This pairing stems from the fact that companies must address growing security concerns, comply with industry and government regulations and empower employees to be more productive in resource-constrained economic times. By aligning these two technologies, businesses can give the employees one touch access to all the information while fully addressing their critical security issues.

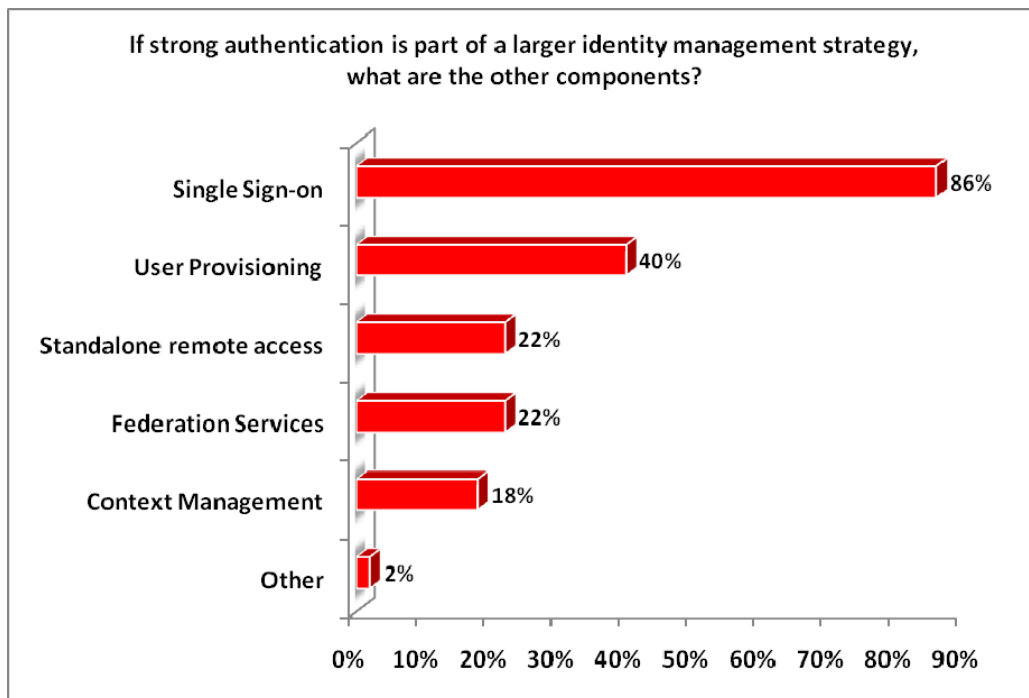


Figure 1

## Strong authentication is no longer being used exclusively for remote access

53 percent of respondents stated that they are currently using strong authentication only for remote access. With insider threats increasing in frequency and intensity, many businesses have left themselves susceptible to a security breach within the organization. Subsequently, 52 percent of respondents stated that they are or have plans to deploy more than one form of strong authentication in order to achieve 360 degree protection from all security threats in their organization, whether employees are accessing data locally or from a remote location.

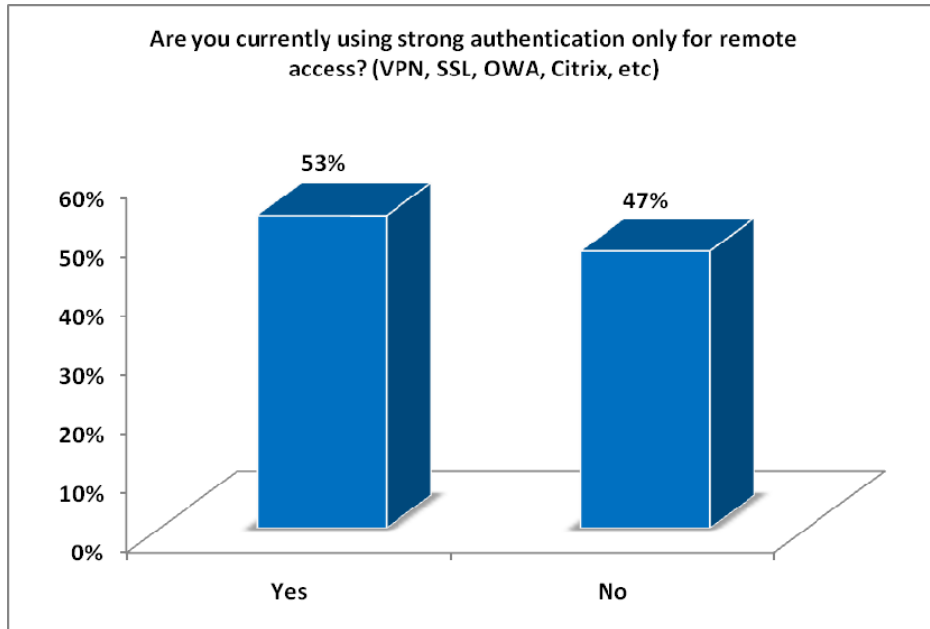


Figure 2

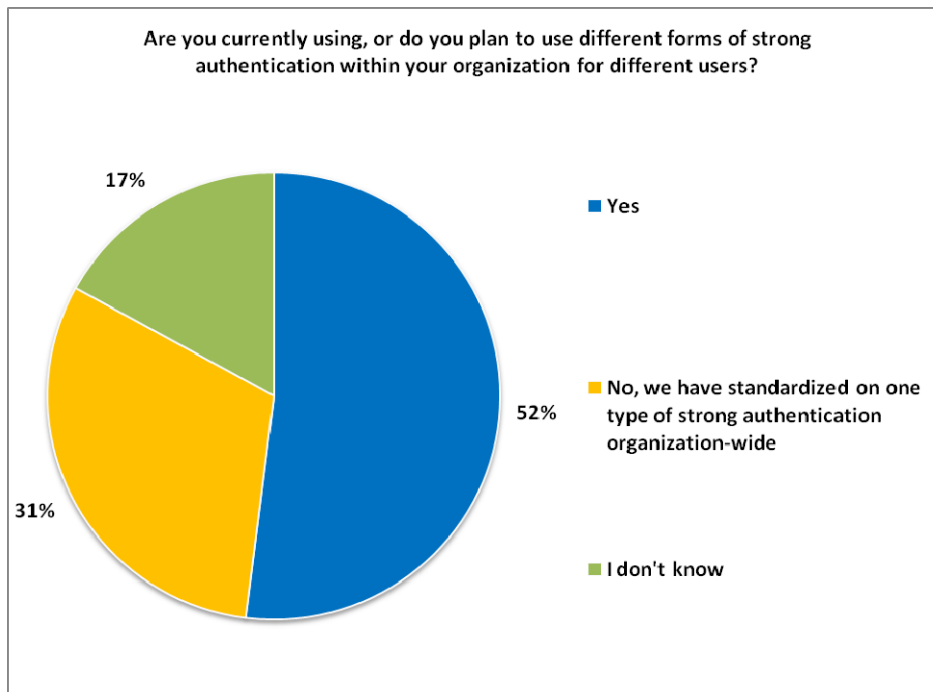


Figure 3

## Companies preferences for strong authentication options changing in order to better match existing employee workflows

While respondents' current strong authentication solutions of choice fall into two distinct groups, device preferences are clearly shifting. This shift is being driven by the ubiquitous nature and low cost of these devices as well as workflow and individual needs which demand a more convenient way for employees to perform their jobs while IT is ensuring data is safe from a potential security breach. Supporting data points include:

When asked what forms of strong authentication they currently have in place, 46 percent of respondents stated facility access badge/proximity card while 43 percent responded OTP token.

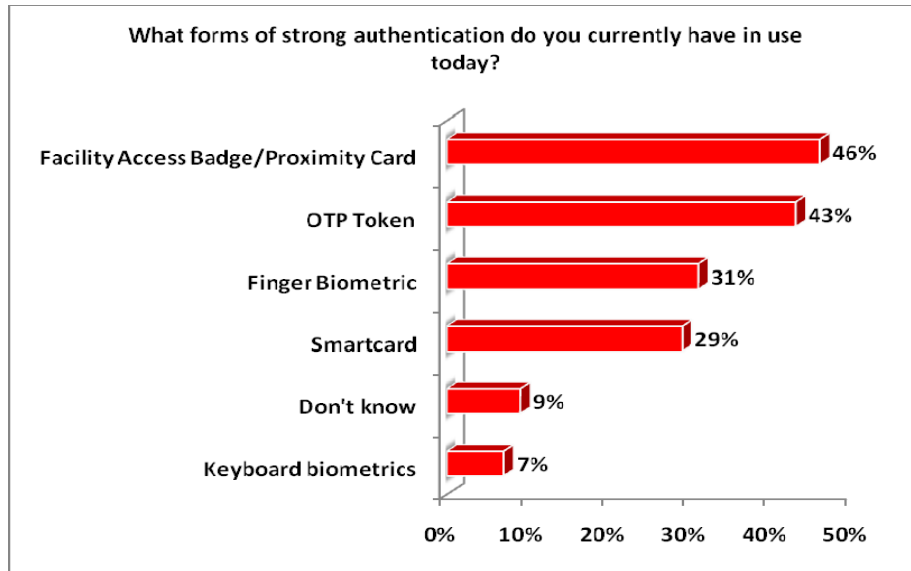


Figure 4

When asked what forms of strong authentication they plan to use, or are investigating for future use, 41 percent of respondents stated fingerprint biometrics and 39 percent responded smartcards. With 28 percent moving to OTP tokens, as compared to the 43 percent, previously stated.

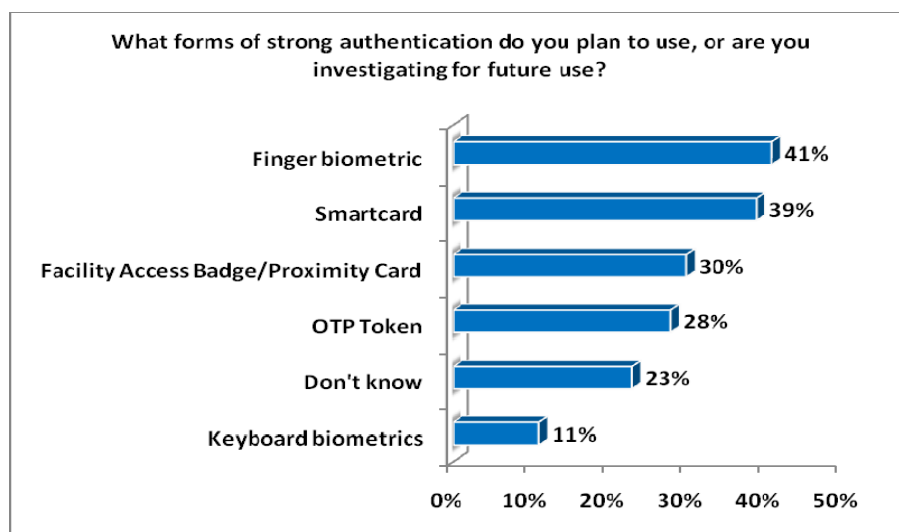


Figure 5

56 percent of respondents stated that they have considered re-using building access cards as strong authentication devices for Windows Logon.

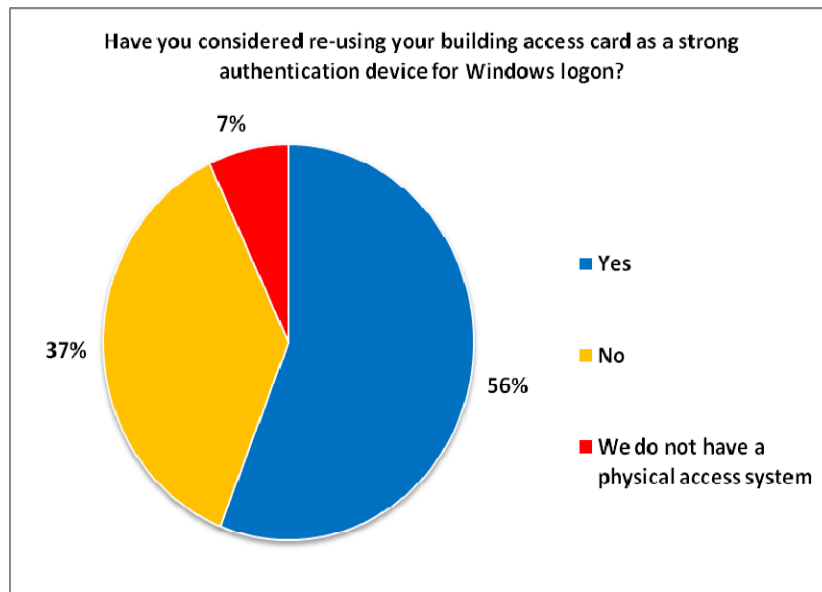


Figure 6

### Companies lack, but want, centralized management and reporting of multiple strong authentication modalities

While the deployment of multiple forms of strong authentication is on the rise, many businesses are unable to centrally manage all from one location without costly integration projects. This creates a highly inefficient process where security teams are forced to manage and track multiple systems or creates additional potential security risk by leaving management tasks up to each individual end-user.

86 percent stated that they currently do not have a way to centrally manage more than one form of strong authentication. Additionally 24 percent of respondents stated that strong authentication management is left up to the end-user.

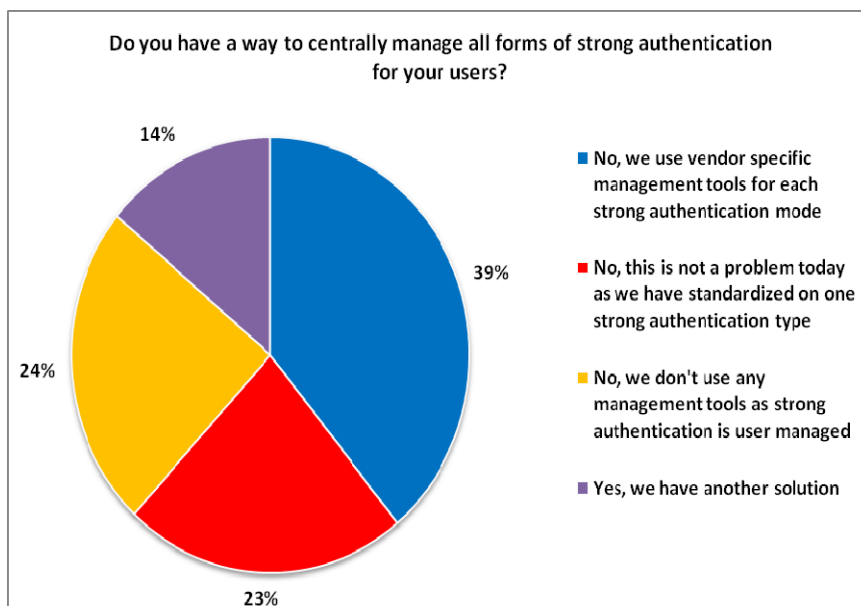


Figure 7

In addition, a significant number of respondents want to track strong authentication access events across their entire organization but according to the survey do not have the proper tools to help them do so at this time.

32% of respondents stated that they would like a central audit log for all users and modes but can't currently find a solution to help in this area.

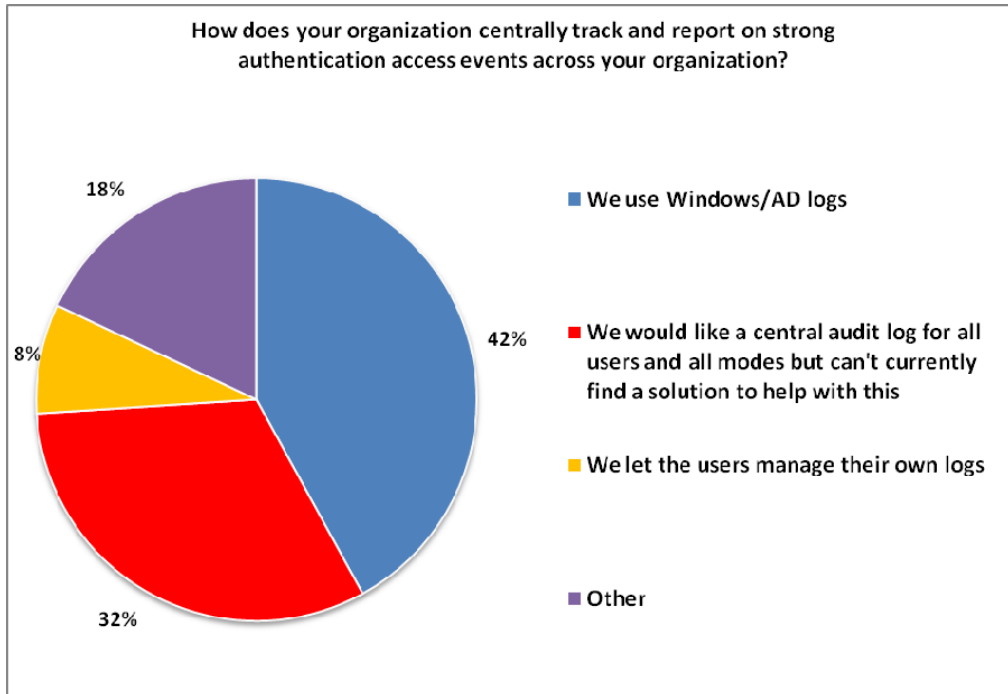


Figure 8

For additional details on strong authentication, including solution benefits and available options please visit: [http://www.imprivata.com/onesign\\_authentication\\_management](http://www.imprivata.com/onesign_authentication_management)

### About Imprivata

[Imprivata](http://www.imprivata.com) secures employee access to desktops, networks, applications and transactions. Its appliance-based, employee access management platform, OneSign, enables organizations to protect enterprise information assets while improving user productivity. By strengthening user authentication, streamlining application access and simplifying compliance reporting across multiple computing environments, customers realize substantial IT Help Desk and administration cost savings, while achieving the security standards they demand.

Imprivata is a recognized leader in Authentication and Access Management, receiving numerous product awards and top review ratings from leading industry publications and analysts. Headquartered in Lexington, Mass., Imprivata partners with over 200 resellers, and serves the access security needs of more than 800 customers around the world. For more information, please visit [www.imprivata.com](http://www.imprivata.com).